SPIDER
SO CYBER RANGE

SPIDER

a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services

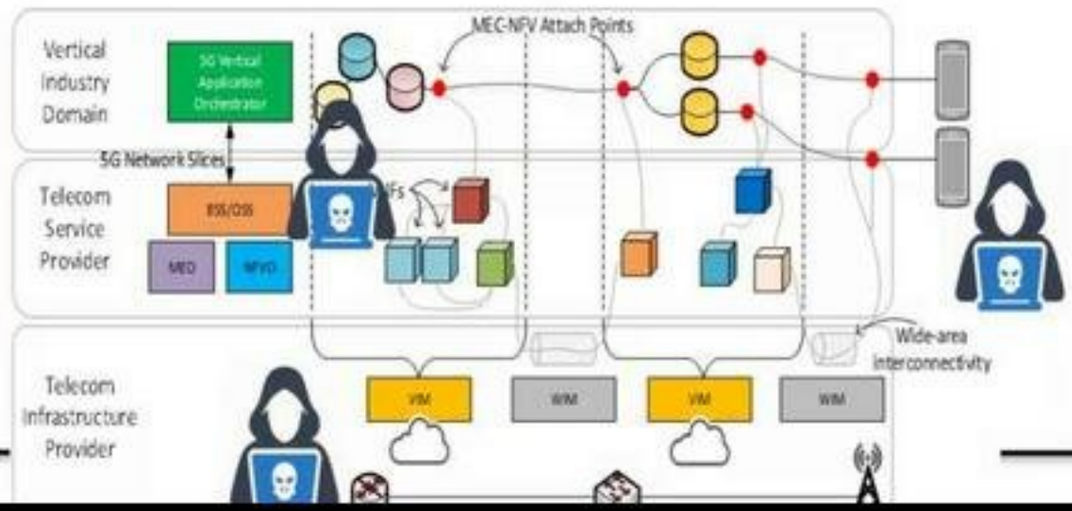
Thursday 26 November 2020

The challenge

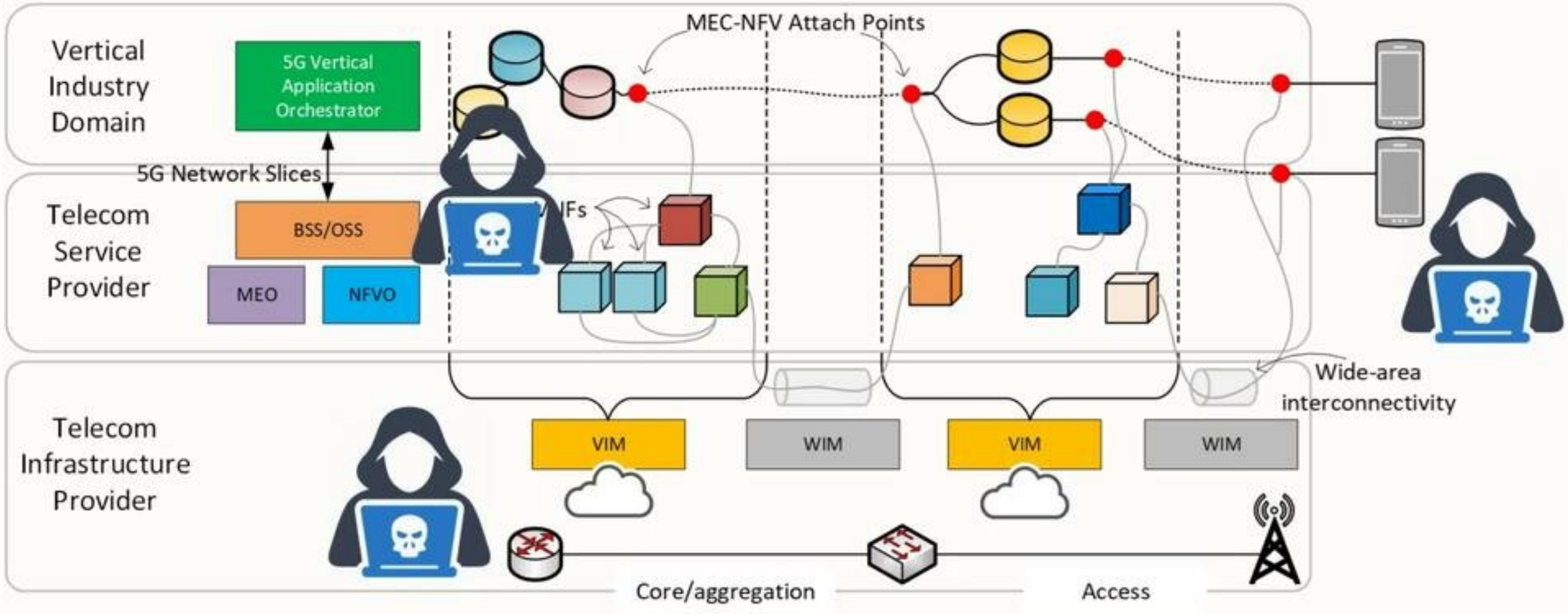
- The emergence of 5G architecture **raised radical changes** in the telco domain
- The **slicing** concept and the **virtualization** of all layers established a **completely new landscape** for both **operators** and application **developers**
- The 'new operational landscape' contributes in the **increase of cyber attack surface**
- 5G incorporates many advanced technologies (e.g. SDN, NFV, SDR, Virtualization) each of which **exposes its own attack surface**

The complexity of today's cybersecurity landscape emphasises the need for **highly competent experts** in securing critical multi-tenant and multi-service environments, such as 5G mobile networks.

5G Threat Landscape



5G Threat Landscape



Concept and approach

Innovative **Cyber Range as a Service platform** that extends and combines the capabilities of existing telecommunication testbeds and cyber ranges with

- latest technologies in **telecommunications management** and **emulation**
- **cyber security training** through **gamification and serious games**
- tools for analysing the **economics of cybersecurity solutions**

Uniquely virtualises as **a single and easily accessible solution**

Three major pillars:

- **cybersecurity testing and assessment**, with emphasis on new security technologies;
- **cybersecurity training** in defending against advanced cyber-attacks; and
- **cybersecurity investment decision support**.

Project Information

SPIDER: a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services

H2020 Project - Work Programme 2018-2020

- **Secure societies - Protecting freedom and security of Europe and its citizens**

Call: H2020-SU-DS-2018

- **Topic**: SU-DS01-2018 Cybersecurity preparedness - cyber range, simulation and economics

Duration: 1 July 2019 - 30 June 2022

The Consortium

SPIDER
SO CYBER RANGE

ERICSSON · cnit · Telefónica · THALES · Atos · UBITECH ubiquitous solutions

POLITÉCNICA · FONDAZIONE BRUNO KESSLER · uni.systems · 8 Bells · FORTH INSTITUTE OF COMPUTER SCIENCE · SERIOUS GAMES INTERACTIVE · UNIVERSITY OF PIRAEUS

CITY UNIVERSITY LONDON · Cyberlens · infalia · InfoCom

19 partners from **9 European countries** (high diversity)

- 5 x Large Industries
- 6 x Research Institutes and Universities
- 8 x SMEs

Goals / Objectives of SPIDER

SPIDER
SG CYBER RANGE

- To **develop** a **Cyber Range as a Service platform** targeting the specifies of **5G infrastructure**
- To **realize** an engine capable of **modelling and emulating** network **services** and **applications** as well as **complex cyber-attacks**
- To **provide active learning strategies** towards increasing the **cybersecurity skills** and **awareness** of **modern cyber defenders**
- To **implement** capabilities for **tracking** the **trainee's activity**
- To **integrate** **cyber range-driven** **risk analysis** and **propose** **econometric modelling tools** capable to forecast the **economic impact of cyber risks**

Target end users & Modalities

- Distinct **Value Proposition** for:
  - **Training Scenario Creators**
  - **Red Team Members**
  - **Blue Team Members**
  - **Infrastructure Providers**
  - **Risk Auditors**
- **Modalities:**
  - **Modality 1: Theoretical Training**
  - **Modality 2: Hands-on Training**
  - **Modality 3: Simulation**

Modality 1: Theoretical Training

SPIDER
SO CYBER RANGE

- **Goal**: Leverage the theoretical background of trainees
- **Medium** : Interactive Tests that aim to infer the level of the trainee regarding Hacking Tactics and Techniques
- **Model-Adherence**: MITRE ATT&CK

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
10 techniques	6 techniques	9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	14 techniques	25 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Boot or Logon Autostart	BITS Jobs	Exploitation for Credential	Browser Bookmark Discovery
Gather Victim	Develop	Services		Boot or Logon		Deobfuscate/Decode		Cloud Infrastructure

Theoretical / Pracitcal Skill Level

Modality 2: Hands-on Training

SPIDER
SO CYBER RANGE

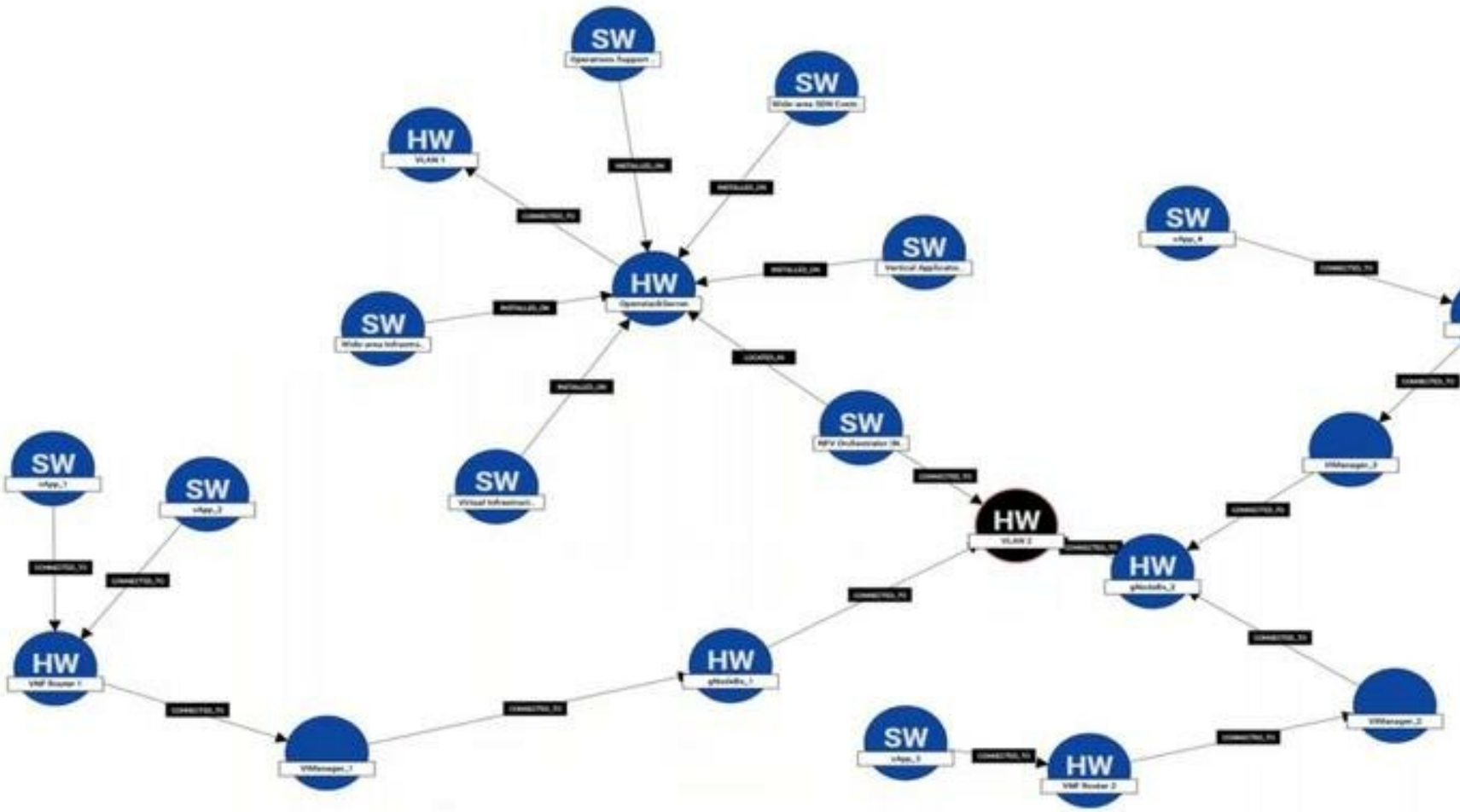
- **Goal**: Leverage the practical skills of trainees
- **Medium** : Setup of a Virtual Infrastructure that covers 5G assets
- **Model-Adherence**: MITRE CAPEC

3000 - Domains of Attack

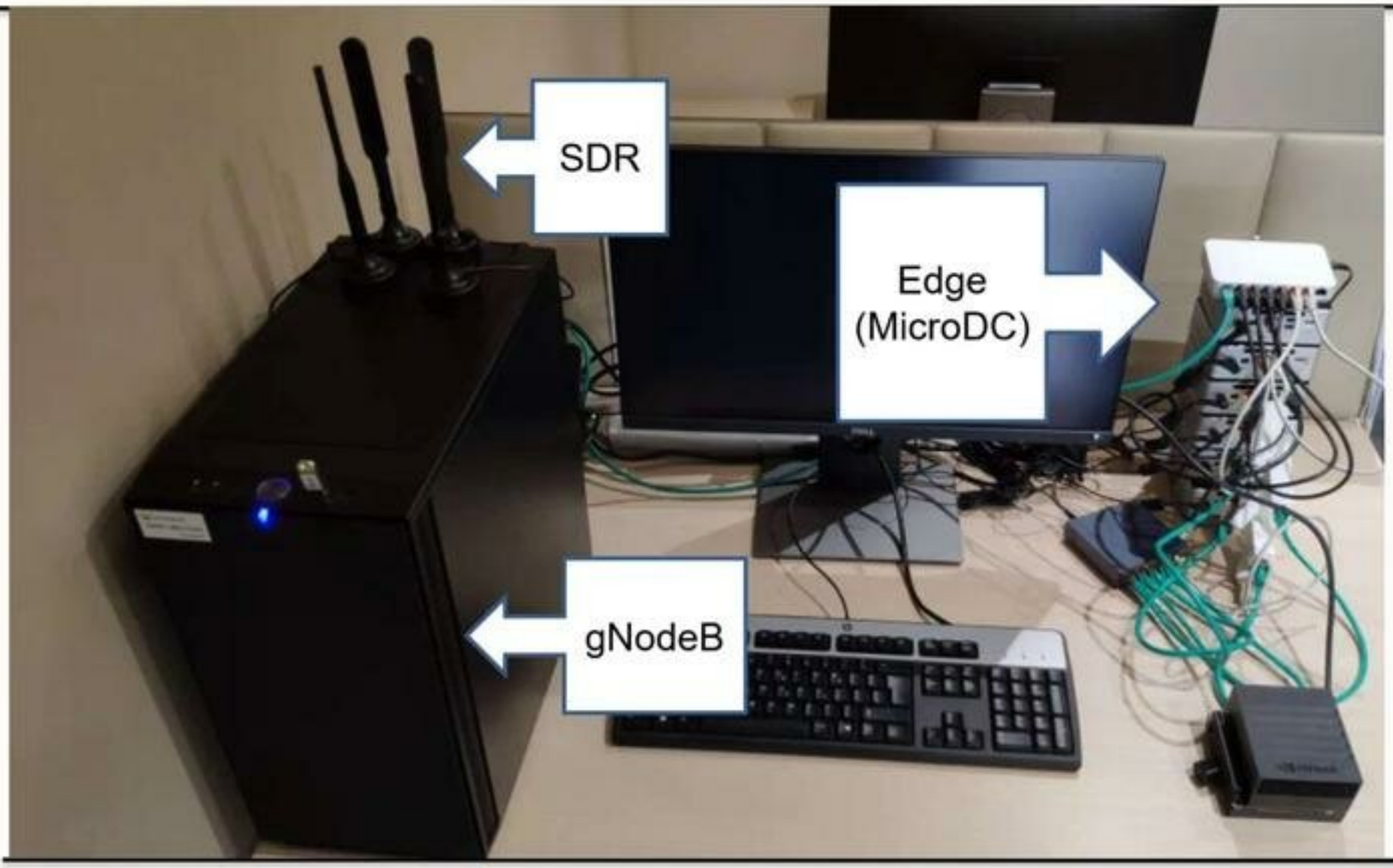
- Software - *(513)*
  - Exploitation of Trusted Identifiers - *(21)*
  - Exploiting Trust in Client - *(22)*
  - Forced Deadlock - *(25)*
  - Leveraging Race Conditions - *(26)*
  - Fuzzing - *(28)*
  - Manipulating State - *(74)*
  - Man in the Middle Attack - *(94)*

Example Instantiated Topology

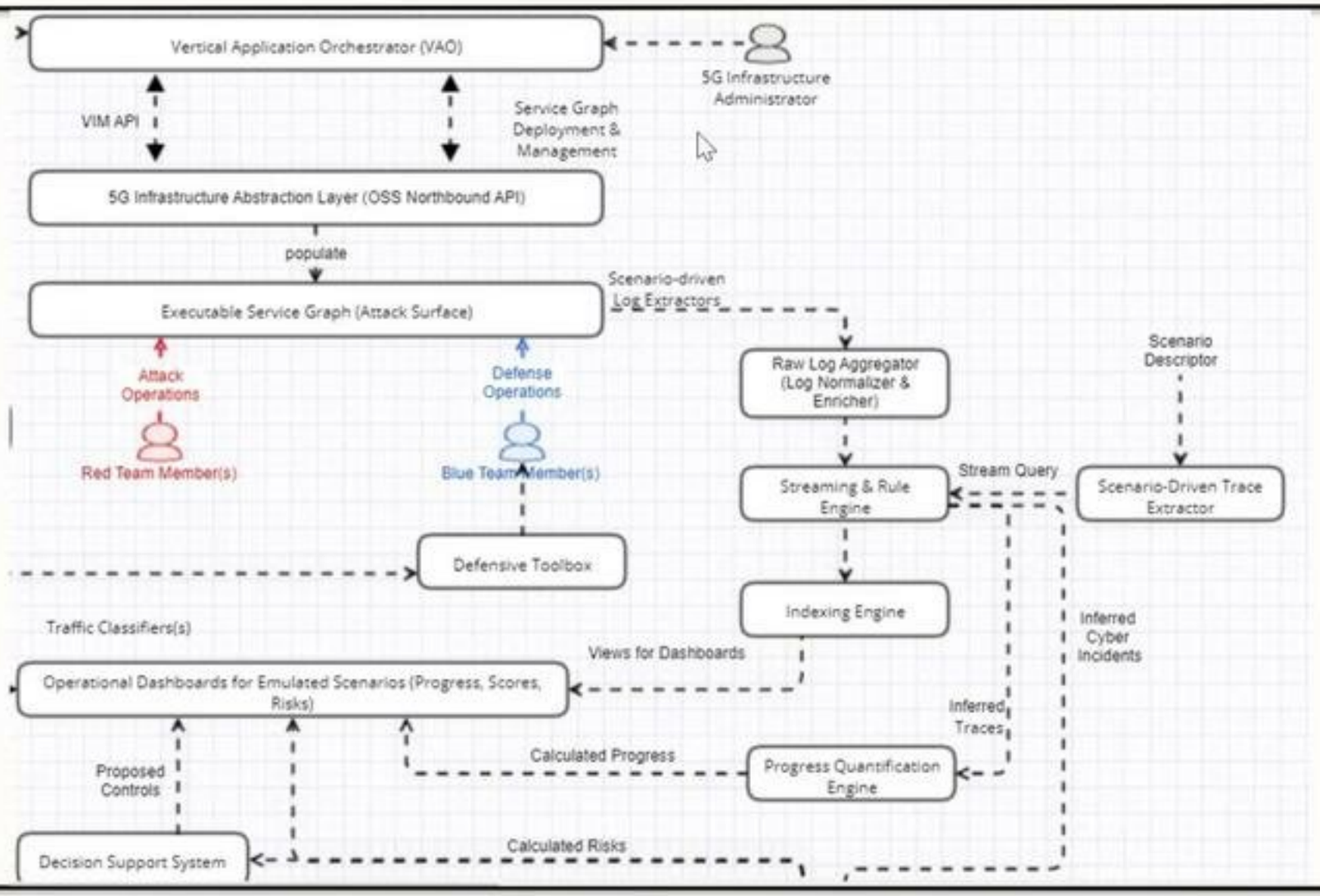
SPIDER
SO CYBER RANGE



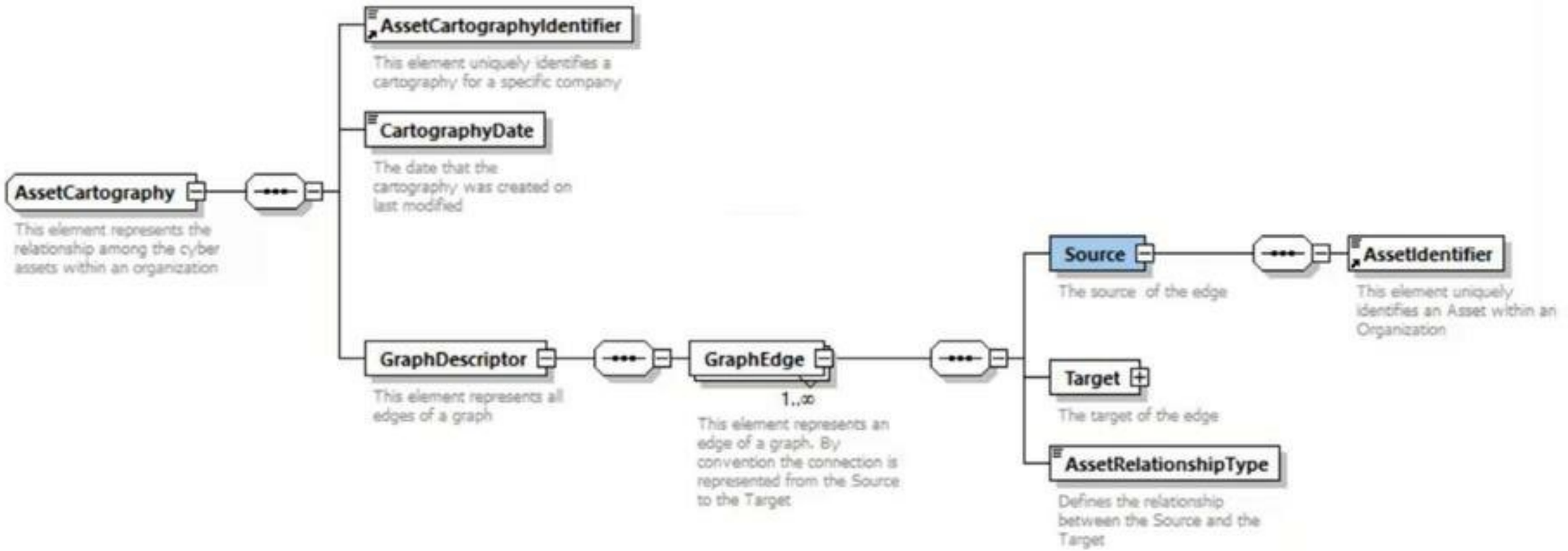
VNFs & PNFs used (4G/5G in a box)



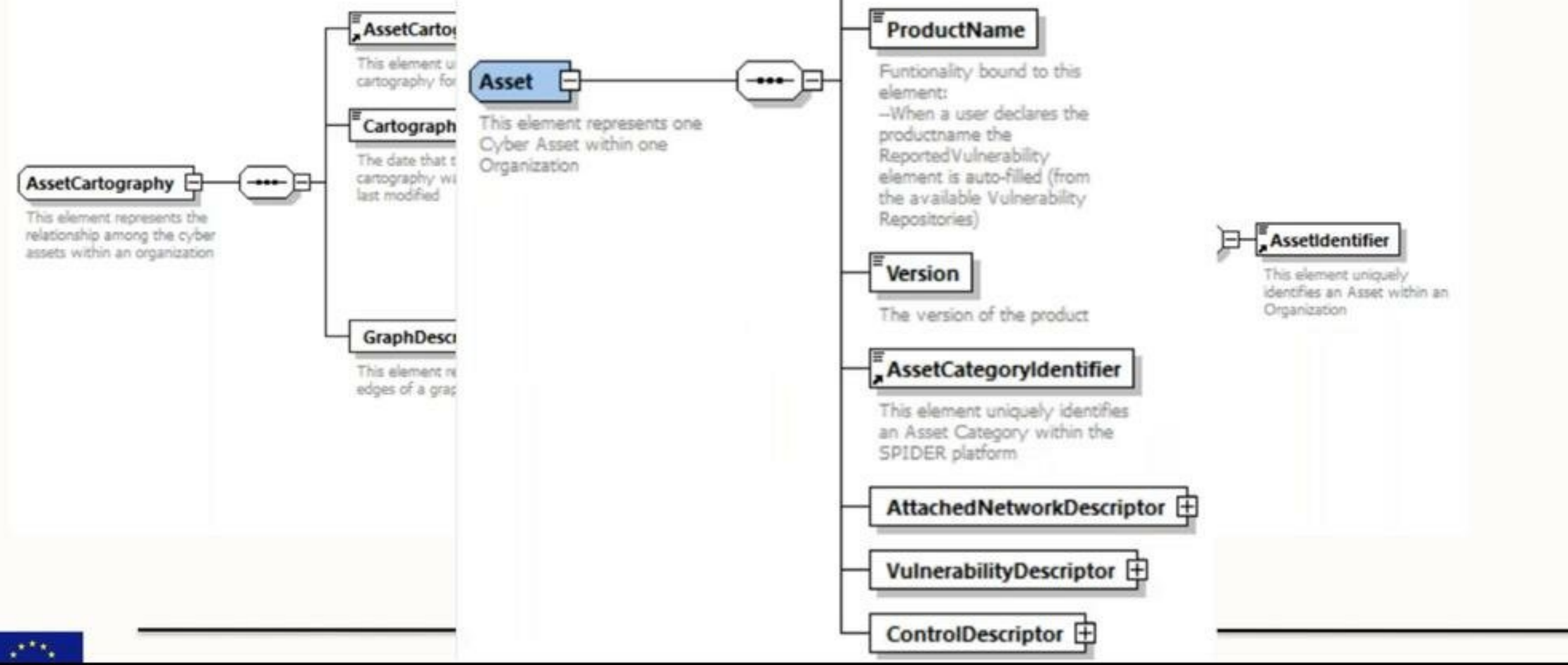
VSOC & Scoring Model



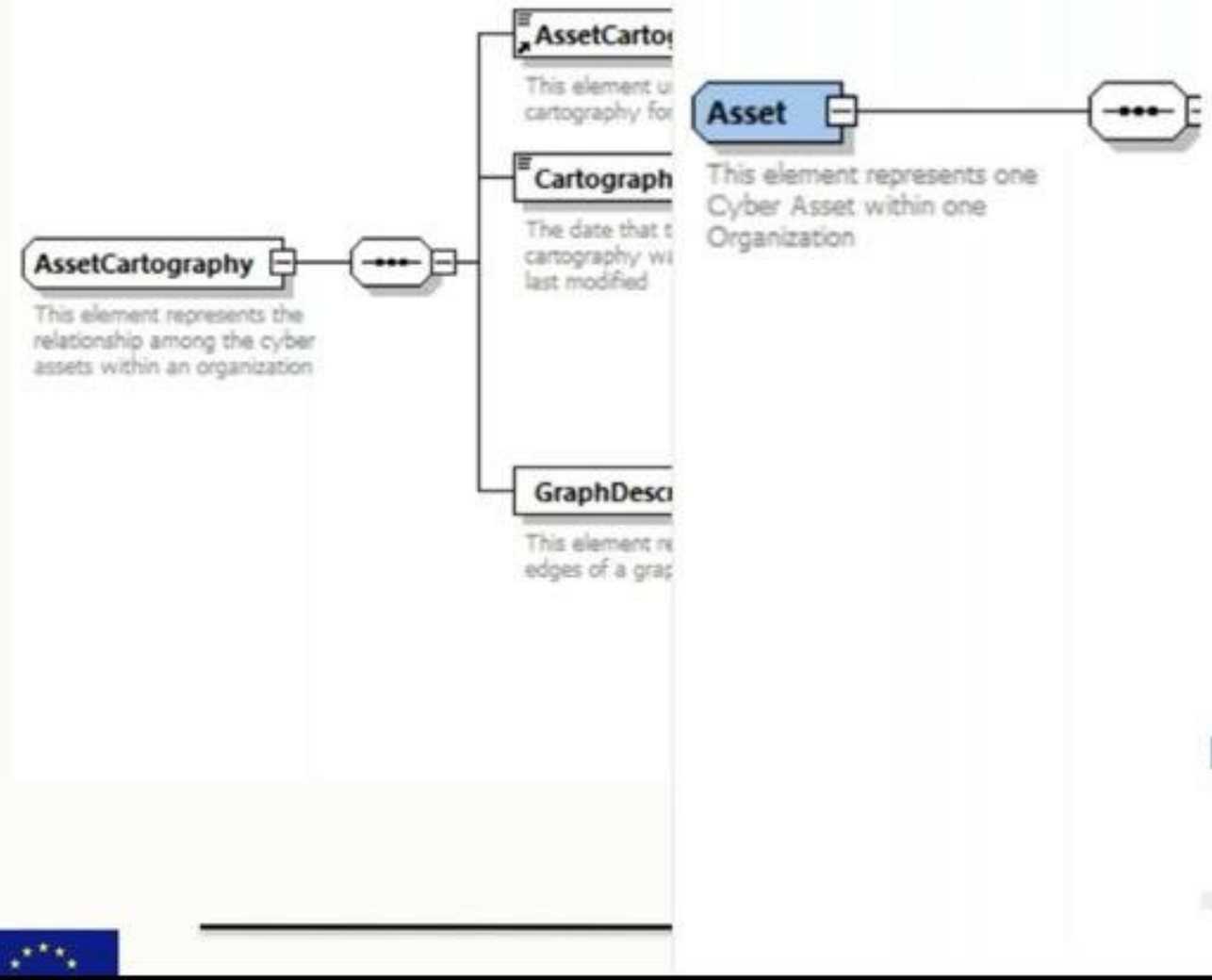
Normative Models



Normative Models

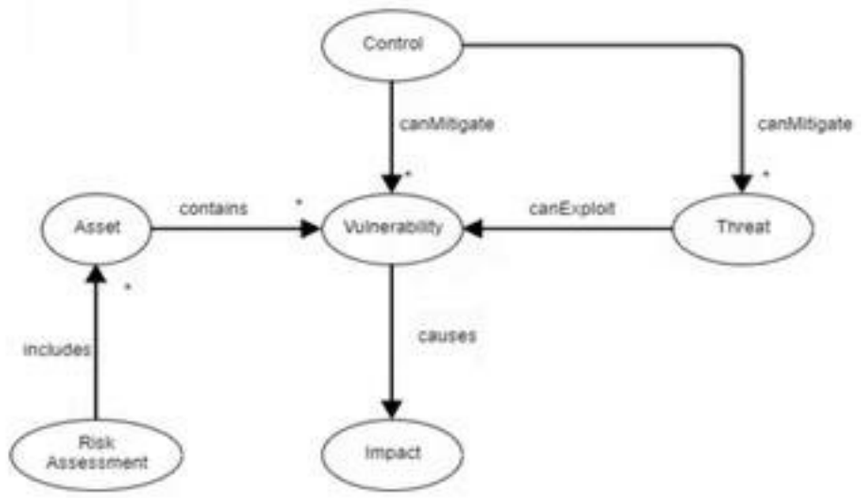


Normative Models



Modality 3: Simulation Training

- **Goal**: Leverage the Risk Assessment skills of auditors/assessors
- **Medium** : Setup of a logical Infrastructure with hypothetical assets and controls
- **Model-Adherence**: NIST Models, CVE, CWE,CPE, ISO-27001

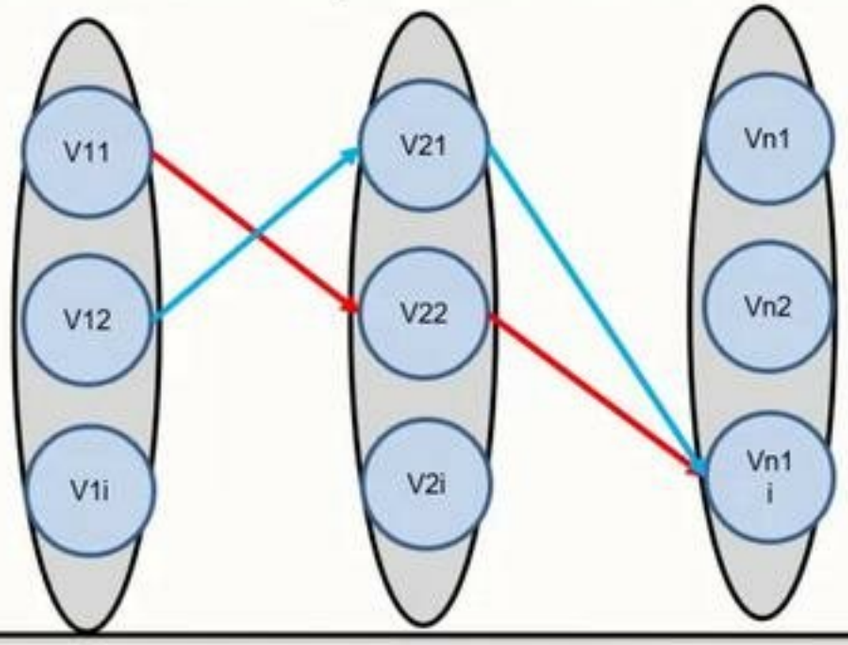


Calculation Model (non Graph-based)

- Individual_Risk = f(VL , IL , TL)
  - TL = f(AV , AC , AUTH)
  - IL = f(C , I , A)
  - TL = subjective
- In traditional models TL is hypothetical
  - Also known as Risk Appetite
- SPIDER provides TL quantification

Calculation Model (Graph Based)

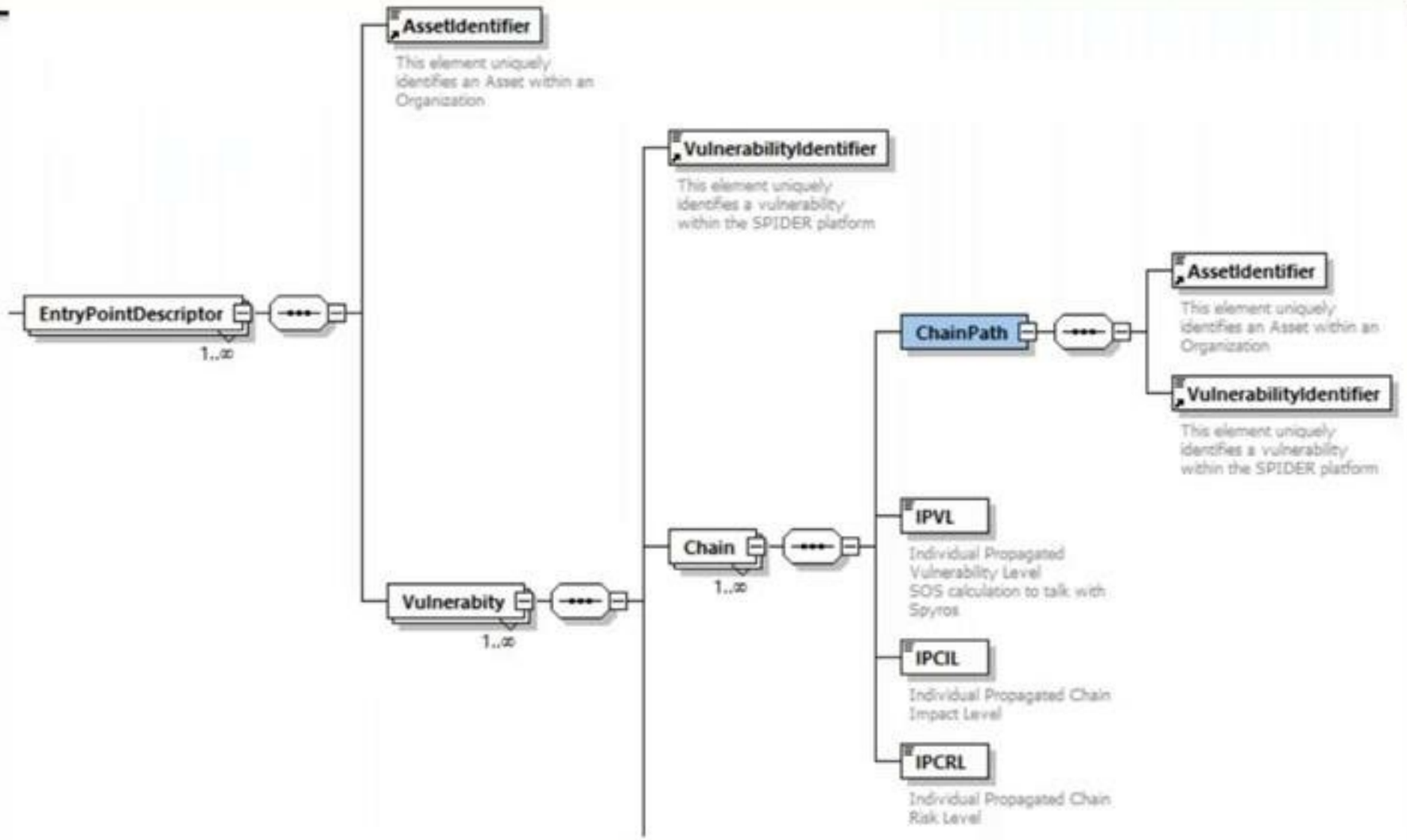
- When Assets are connected model is bound to the Direct Acyclic Graph;
  - Individual Risk Level **IRL**
  - Propagated Risk Level **PRL**
  - Cumulative Risk Level **CRL**
- Both PRL and CRL are dependent to Attack Paths



Game Definition

- What is defensive strategy that has to be followed with given:
  - Asset (vulnerable) topology
  - Likelihood per Attack
  - Acceptable Risk
- Defensive strategy is set of **controls** under a given “cost”

Normative Models



Takeaways

- SPIDER is a “niche” Cyber Range platform targeting the specificities of the 5G telco domain
- It offers three distinct learning-modalities
- It follows de-facto standards
- It exposes normative APIs and structures for its artefacts

Major Challenges

- Syntactic Interoperability of Scenarios
- Model alignment (skills, topologies)
- Scoring models

SPIDER
SO CYBER RANGE

Thank you!


FORESIGHT
Advanced cyber-security simulation platform for preparedness training in Aviation, Power-grid and Naval environments
Cyber Range Network
Joint Webinar
KEMEA-UOP
Dimitrios Kavallieros (Project Coordinator)
Nicholas Kolokotronis (Technical Coordinator)
Cyber Range Network Joint Webinar
26/11/2020
This project has received funding from the European Union's Horizon 2020 Research and Innovation Action under Grant Agreement No 833673.

FORESIGHT

Advanced cyber-security simulation platform for preparedness training in Aviation, Power-grid and Naval environments

Cyber Range Network

Joint Webinar

KEMEA-UOP

Dimitrios Kavallieros (Project Coordinator)
Nicholas Kolokotronis (Technical Coordinator)

Cyber Range Network Joint Webinar

26/11/2020

This project has received funding from the European Union's Horizon 2020 Research and Innovation Action under Grant Agreement No 833673.

General information

FORESIGHT

H2020-SU-DS-2018 SU-DS01-2018 Innovation Action

Topic SU-DS01-2018 "Cybersecurity preparedness – cyber range, simulation and economics"

DURATION: 10/2019 – 09/2022

GRANT Agreement No. 833673

- 22 partners
- 9 EU member states
- Overall budget ≈ 7,3 m
- Actual budget ≈ 5,9 m

Partners

FORESIGHT

Project Coordinator

KEMEA

Partners

European Dynamics

Information Technologies Institute

Cybercrime Research Institute

inCITES Consulting S.A.R.L.

CENTRIC Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research

MINDS & SPARKS

Abertay University

AIRBUS

OPEN UNIVERSITY OF CYPRUS

ECOLE NAVALE

CYBEXER TECHNOLOGIES

ATHENS

THALES

РАЗПРЕДЕЛЕНИЕ

CERT.BG

ieit

ESO

University of Strathclyde Glasgow

UNIVERSITY OF PORTSMOUTH

FORESIGHT motivation

FORESIGHT

- ✓ Rapid growth of new forms of cyber-attacks that are quite hard to forecast, detect, mitigate, but also to recover
- ✓ The need for the development of innovative ways to implement security measures
- ✓ Security technology market fragmentation in cyber-defense systems
- ✓ Security skills' shortage
- ✓ Lack of security executives' deep awareness of cyber-security risks

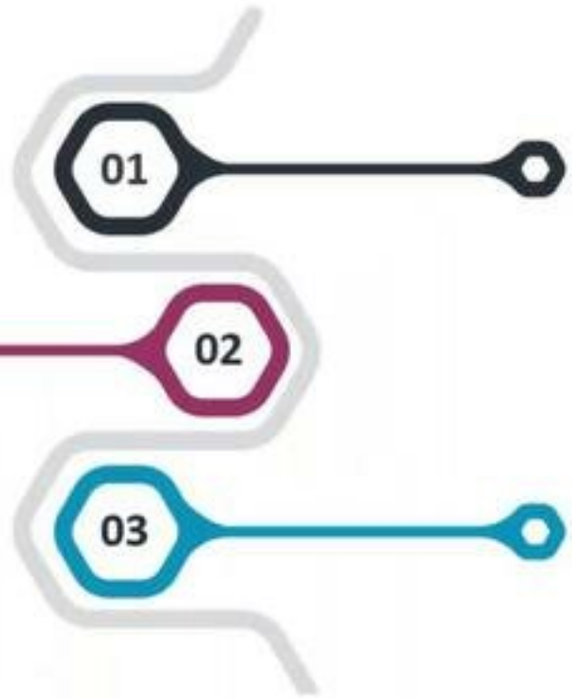
- ✓ Highly skilled cyber-security professionals are needed by the industry
- ✓ Cyber security training should be a continuous learning process
- ✓ Advancements in realistic, diverse, and dynamic simulation environments

FORESIGHT scope

FORESIGHT

complex cross domain/hybrid scenarios

Extend the capabilities of existing cyber-ranges and will allow the creation of complex cross-domain/hybrid scenarios to be built jointly with the IoT domain



Federated cyber range

Develop a federated cyber-range solution to enhance the preparedness of cyber-security professionals at all levels and advance their skills towards preventing, detecting, reacting and mitigating sophisticated cyberattacks

ecosystem of networked realistic training and simulation platforms

Deliver an ecosystem of networked realistic training and simulation platforms that collaboratively bring unique cyber-security aspects from the aviation, smart grid and naval domains

FORESIGHT Objectives

CREATE a state-of-the art platform that will greatly extend the capabilities of existing cyber-ranges by allowing them to be a part of a cyber-range federation.

DELIVER training curricula aimed at cyber-security professionals to implement and combine security measures in innovative ways.

DEVELOP realistic and dynamic scenarios based on identified and forecasted trends and needs in terms of cyber-attacks and vulnerabilities.

INCREASE the dynamics of training and awareness methods in order to match or even exceed the rate of evolution of cyber-attackers.

IDENTIFY the impact of cyber-risks and the most appropriate security measures to protect valuable assets, minimise costs and recovery time.

IMPROVE the number of talented cyber-security professionals to meet the industry's current needs at all levels (from junior to senior).

CR Federation Concept

As defined in ECSO WG5 paper (Mar. '20)

A federated CR solution that

- agrees upon standards of operation (scenario/capabilities description language) in a collective fashion
  - can request provisioning of CR services within the federation
  - each CR to implements/delivers them in own specific way
- complex and costly capabilities and functionalities are shared to achieve multiple UCs

Typically, can also encompass the *integration concept*, in which peer CRs

- communicate with each other to deliver a scenario / simulation ENV spread across them
- plan the integrated network environment (IP address spaces, etc.)

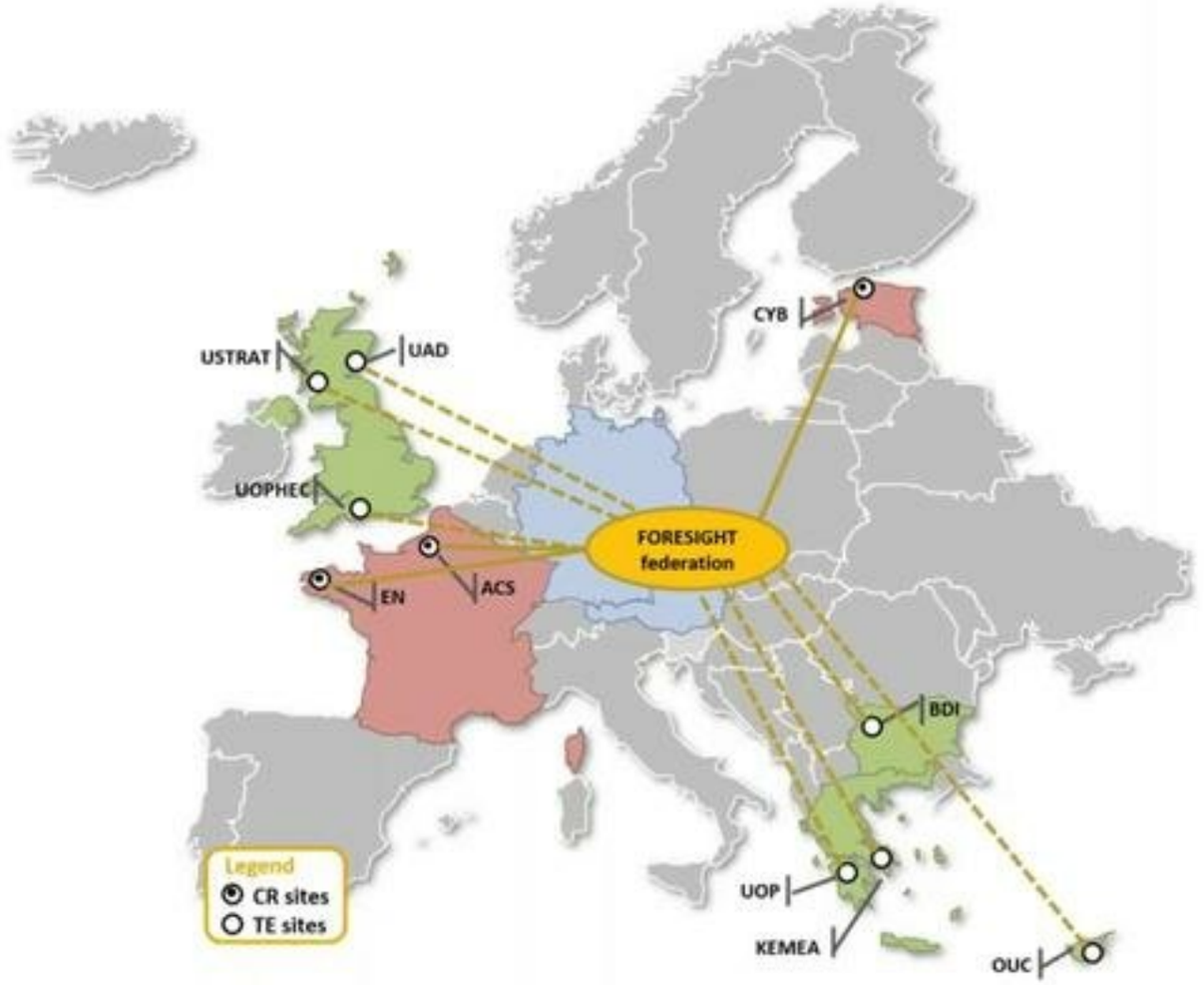
FORESIGHT federation platform for CRs/TEs

FORESIGHT CRs:

- 3 different Cyber Ranges from two different countries: **CybExer** from Estonia, **Airbus** and the **French Naval Academy** from France.
- Developed for different domains but provide training regarding cyber security preparedness and incident response to cyber security experts.

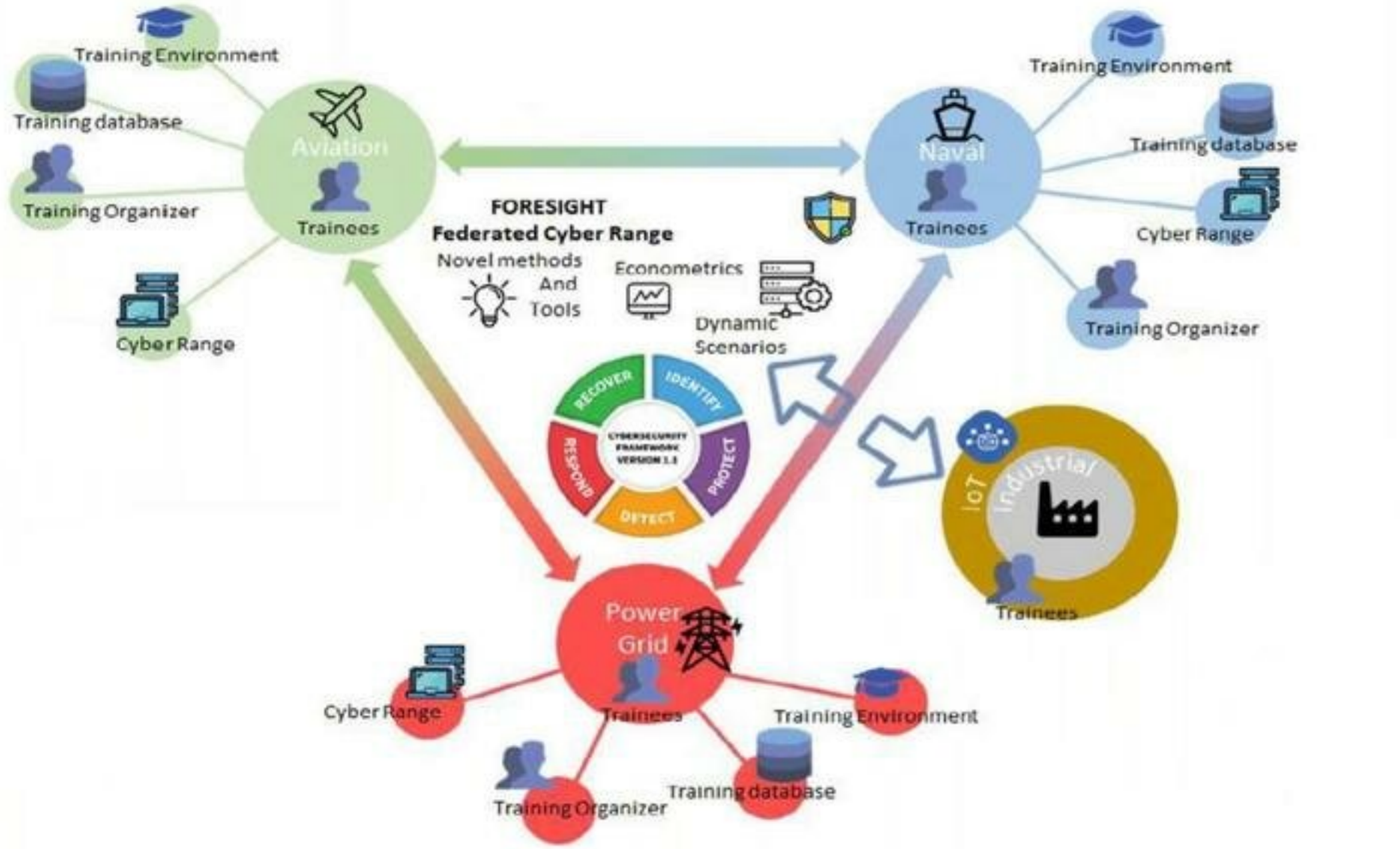
FORESIGHT TEs:

- 6 Technical Experts from 4 different countries.
- Used to train and educate the next generations of cyber security experts in the fields of
  - penetration testing
  - digital forensics
  - malware analysis
  - vulnerability identification
  - patching and incident response



FORESIGHT high-level concept

- Aviation
- Power grid
- Naval
- Hybrid/IoT



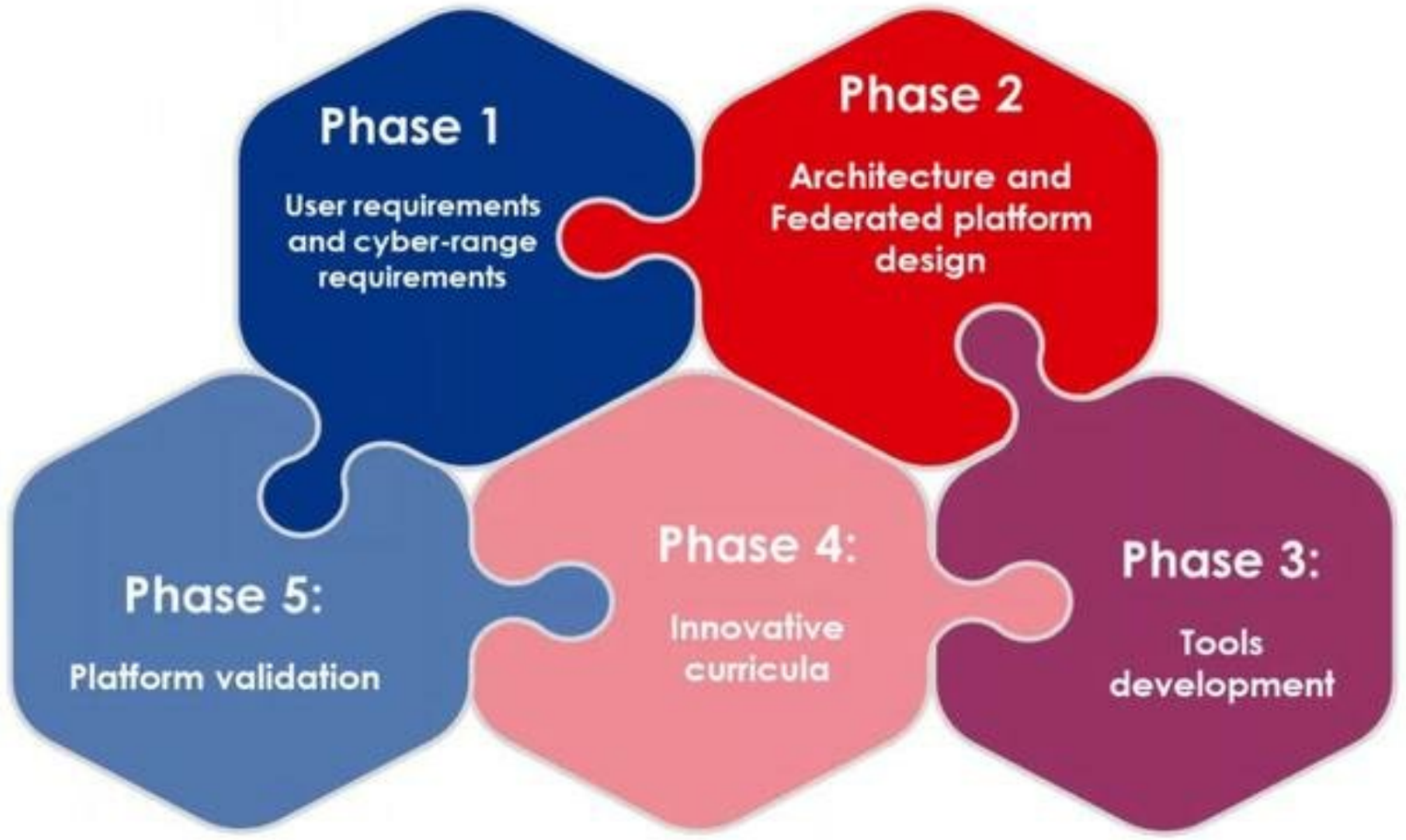
FORESIGHT Federation Approach

FORESIGHT

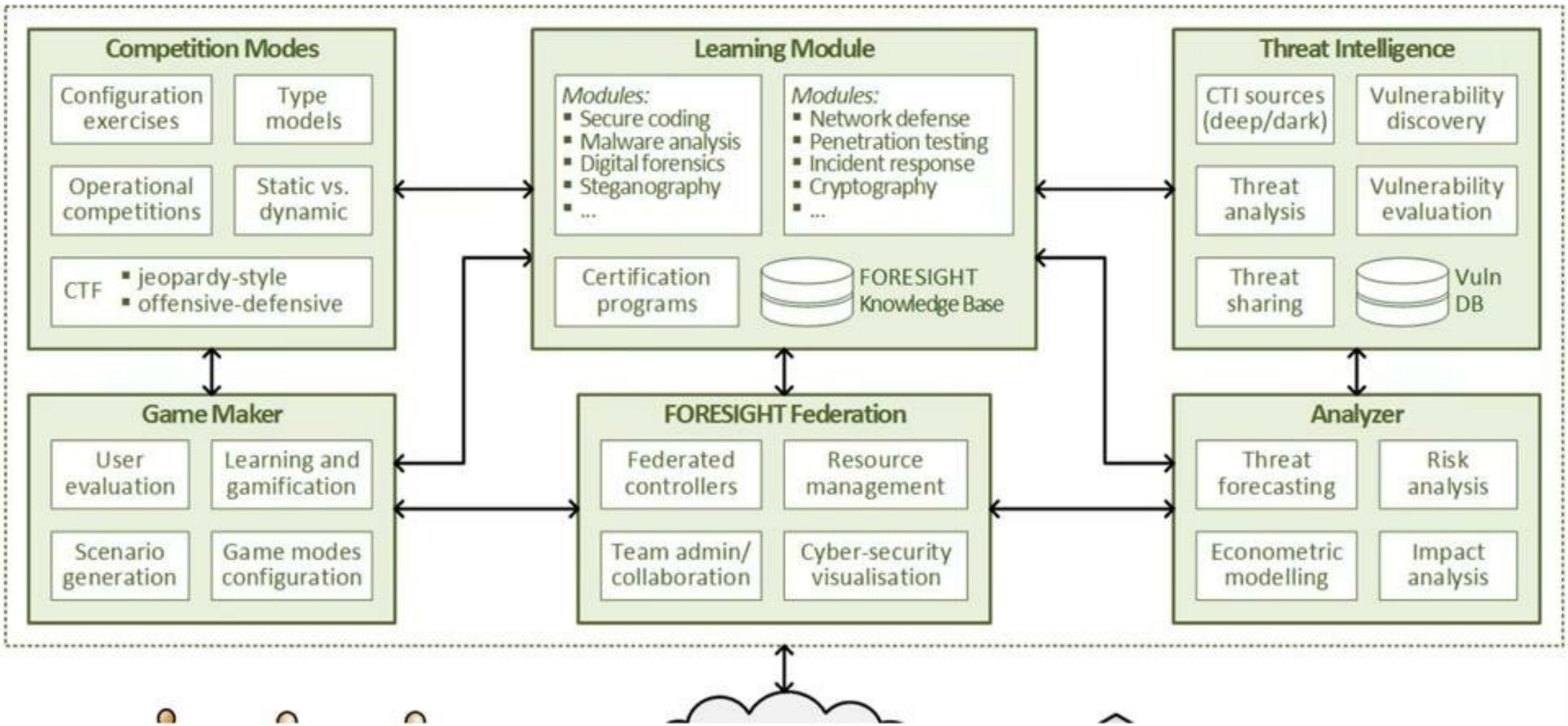
A federated CR solution that

- brings together unique cyber-security aspects from each domain
- considerably extends the capabilities of existing CRs by … allowing complex cross-domain (i.e. hybrid) scenarios to be built
  - … interactions with the much wider IoT ecosystem
- meets the most demanding REQs in terms of ecosystem modelling complexity and training needs
- caters multi-domain training requirements by allowing CRs to connect to each other
- makes available to users a wider range of educational services and material, allowing them to obtain training regarding a broader spectrum of cyber-attacks
- advances the skills of cyber-security professionals … while providing a series of unique features and services (like threat forecasting, risk evaluation, econometric models, etc.)

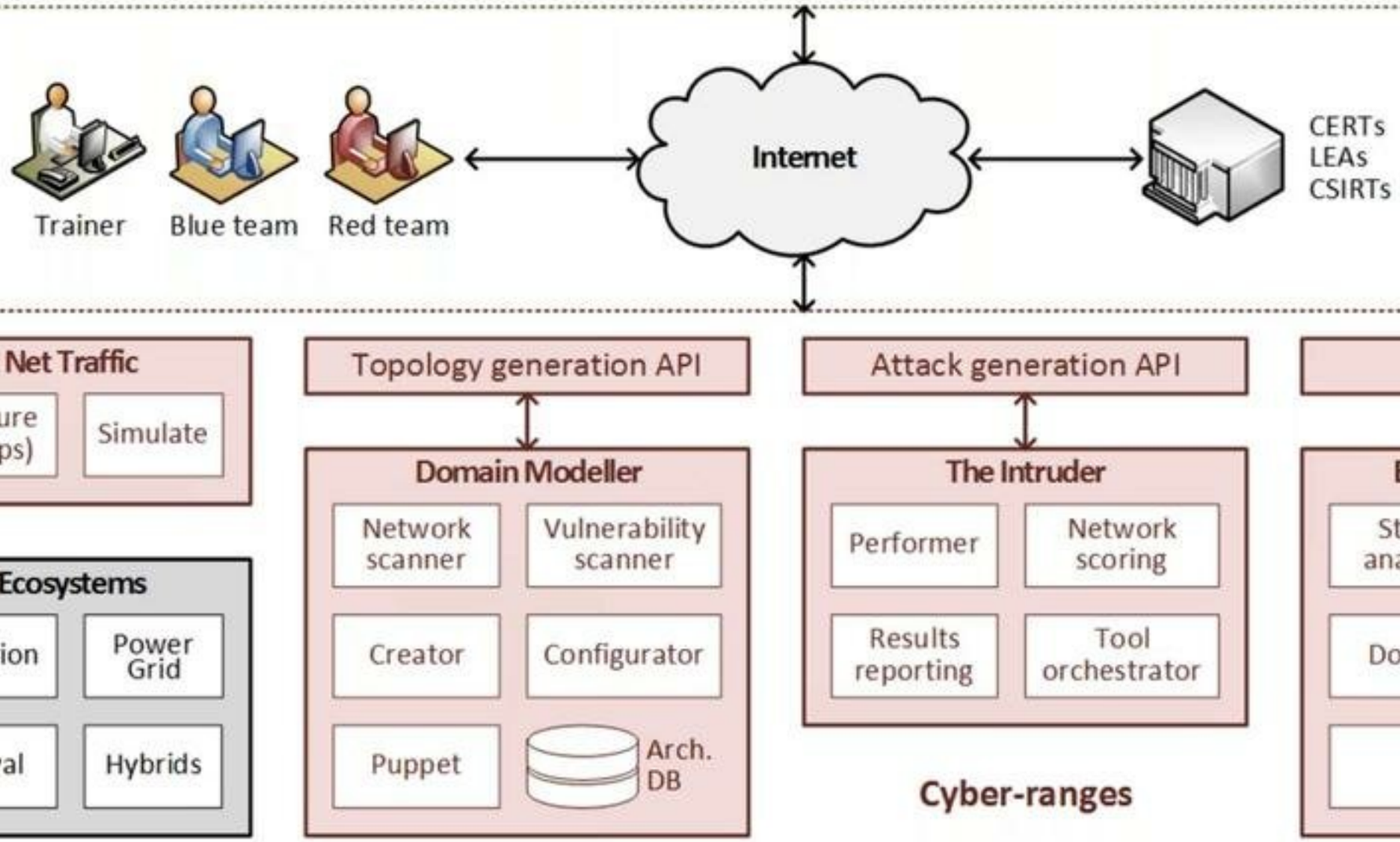
FORESIGHT methodology



FORESIGHT high-level architecture

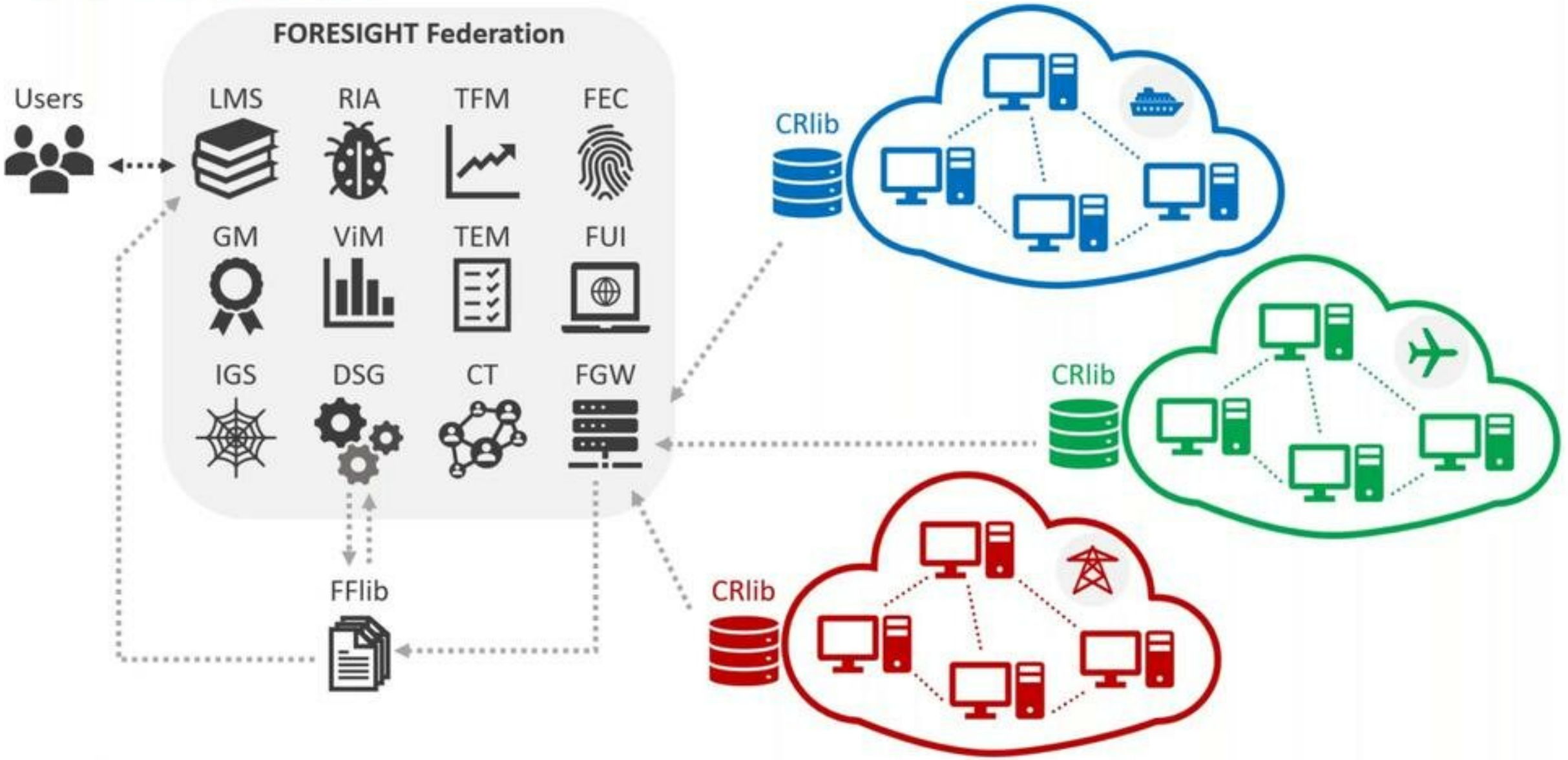


FORESIGHT high-level architecture



FORESIGHT Federated Platform

Cross-domain **and Dynamic** Aspects



FORESIGHT Training and Certification

Main pillars

Individual skills for standalone cyber-security techniques

Team skills for cooperation and communication, both within organization and with external, collaborating organizations

Skills to interact with and benefit from expertise from specialized security bodies (CSIRTs)

Varying levels of difficulty	Real-world attacks scenarios
Different training modes	Deal with the many facets of cyber-security
Certification based on standards	Scalable, cost-effective and easy to use Programs

FORESIGHT Innovation potential (1/2)

FORESIGHT Innovation potential (2/2)

The cyber range market is expected to grow even more in coming years.

Advances in cyber-security econometric model generation.

Several new cybersecurity related jobs will be generated in the future.

Current CRs do not consider the collection of CTI from Dark Web, social media and forums.

Opportunities

Existing CR platforms are not focused on creating the multi-domain training requirements.

Existing technologies of analysis and sharing of CTIs do not utilise online sources (Surface and Dark Web, social media, forums).


THANK
YOU
MERCI
MULTUMESC
GRAZIE
MAAKE
ASANTE
KIITOS
VINAKA
WELALIN
ARIGATO
OBRIGADO
MATONDO
SPASIBO
DANK JE
KIA ORA
JUSPAXAR
MATUR NUWUN
CHOKRANE
TERMA KASIH
RAIBH MAITH AGAT
CAM ON BAN
UA TSAUG RAU KOJ
MOCHCHAKKERAM
NIRRINGRAZZJAK
MAMANA
DANKON
MULTUMESC

SHOW TASKBAR | DISPLAY SETTINGS | END SLIDE SHOW

00:01 | 12:50

Cyber-MAR Overview

Next slide

No Notes.

Slide 1 of 19

Cyber-MAR Overview

About | Project Facts

Title: Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain.

Topic: SU-DS-2018: Cybersecurity preparedness-cyber range, simulation and economics

Contracting Authority: European Commission H2020

Project ID: 833389

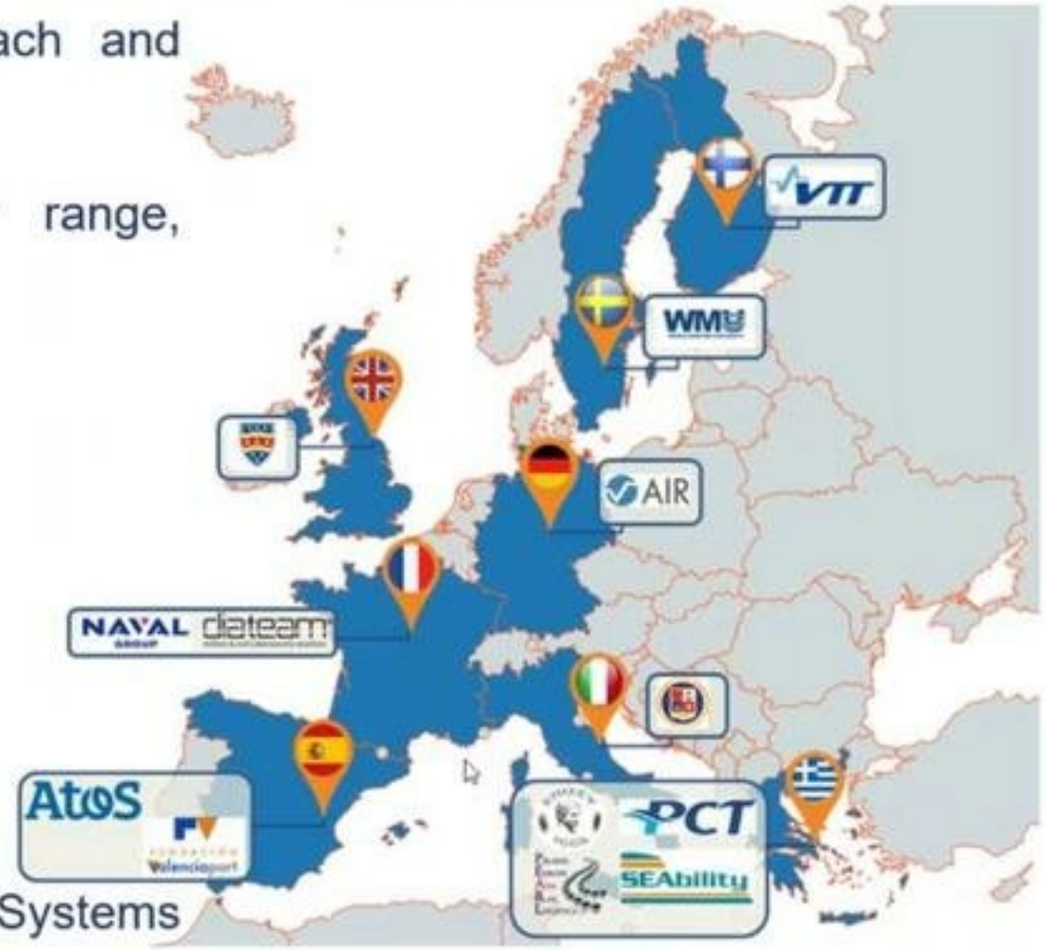
Funded scheme: IA – Innovation Action

Duration: From 2019-09-01 to 2022-08-31

Total cost: EUR 7 154 505.00

EU contribution: EUR 6 018 367.507

Coordinator: Institute of Communication and Computer Systems (ICCS), Greece



Challenges & Goal

- **Maritime information systems** in many cases designed without accounting for the **cyber risk**
- **Digital infrastructure** has become essential & critical to the **safety** and **security** of shipping and ports
- Importance of **handling cyber preparedness** as a highly prioritized aspect is paramount
- Estimation of accurately cybersecurity investments based on valid risk and econometric models

Cyber-MAR ultimate goal unfolds in **two main directions**:

Establishing a "**cyber ecosystem for preparing of cyber attacks**"

Estimating the **impact of cyber-attack** from a financial perspective and supporting the **undertaking of prompt decisions**

Cyber-MAR Key Objectives (1/2)

O1. Enhance the **capabilities** of cybersecurity professionals and **raise awareness** on cyber-risks

Deploy Cyber-MAR Range, training modules through LMS, improvement in response times in specific resilience metrics

O2. Assess cyber-risks for operational technologies (OT)

Maritime Cyber-Risk Assessment deployment and integration in Cyber-MAR platform

O3. Quantify the **economic impact** of cyber-attacks across different industries with focus on **port disruption**

Quantify economic risk in terms of Time-to-Recover or Product Value at Risk, integration in Cyber-MAR platform

Cyber-MAR Key Objectives (2/2)

O4. Promote **cyber-insurance market maturity** in the maritime logistics sector (adaptable to other transport sectors as well)

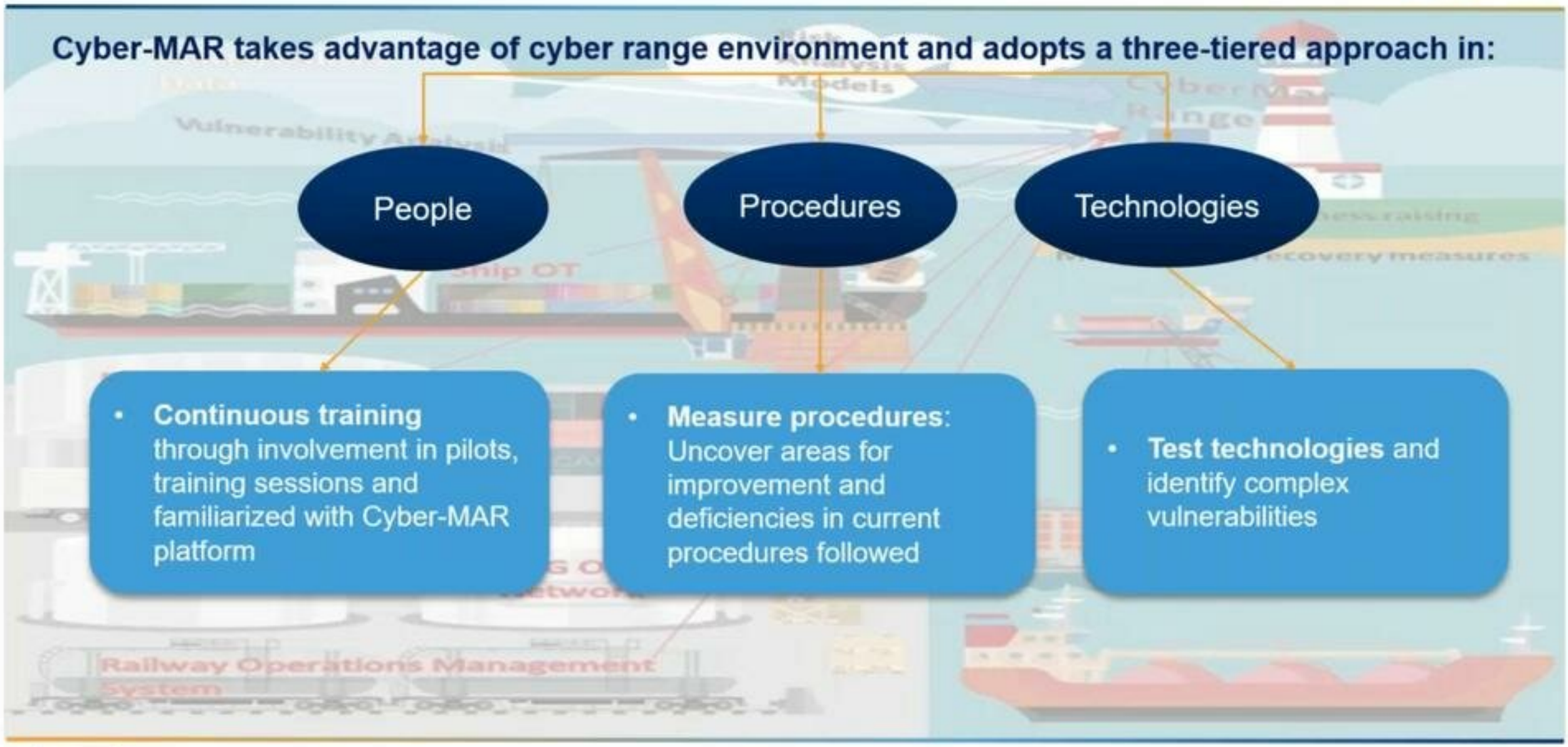
Develop recommendations based on findings and outcomes from Cyber-MAR pilots and simulations

O5. Establish and **extend** CERT/CSIRTs, competent authorities and relevant actors **collaboration** and **engagement**

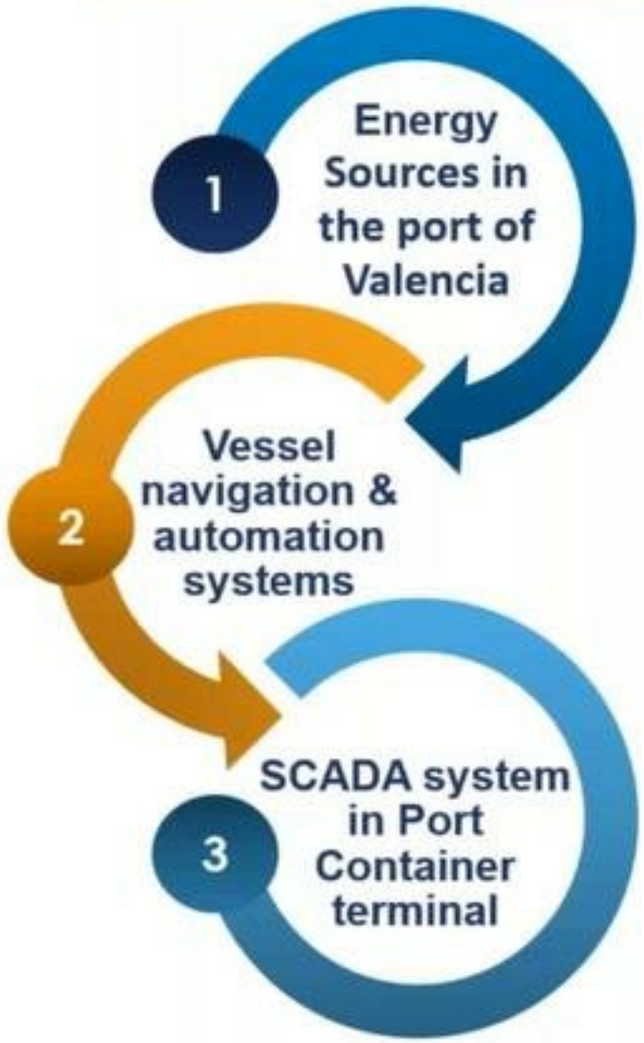
Create a maritime Malware Information Sharing Platform (MISP) community, engage at least 2 CERT/CSIRTs in pilot activities

Cyber-MAR Concept & Methodology

Cyber-MAR takes advantage of cyber range environment and adopts a three-tiered approach in:



Pilot Scenarios



The Cyber-MAR platform will be applied to simulate **the port electrical grid of the port of Valencia**, including protocols for protecting the grid and crisis management after attack.

The Cyber-MAR platform will be applied to simulate **a ship bridge cyber-attack**, including potential attacks to navigation, communication and control systems.

The Cyber-MAR platform will be applied to simulate **a SCADA attack to the Port Container Terminal of Piraeus Port**. In particular, the consequences of a cascade effect extending the attack to the railway operator network.

Expected Impacts

Impact on Resilience to Cyber-Threats & Data Privacy Breaches

Enhancement of the **resilience of target organizations** to new and emerging threats through the **identification of recurring or emerging patterns of cyber-attacks** and **privacy breaches** with a decent degree of accuracy.

Impact on Supply Chain Efficiency

Cyber-MAR aims to offer the potential to **big players of logistics domain** to **join forces on estimating cyber-risk** and **mitigate** such **threats**, while **fostering open tools** that will improve the internal processes within each organization.

Impact on Appropriate Investments for Cyber-Security

Cyber-MAR focuses on the provision of a fully customizable and tailored view on the trade-offs, aims to **increase the available open tools** in number and variety, while offering an **intuitive integration to all** (physical and virtual) **IT components**.

Societal Impact

Cyber-MAR overemphasizes the importance of **accessible training infrastructures for cyber-defense**, in OT, transport and logistics domains and at the same time aims to contribute to the **standardization efforts** to make such issues prominent in the society.

Cyber-MAR Target Audience

- Decision Makers, Public Authorities and International Organizations
- Academia
- Port authorities, operators and associations
- Freight transport and Logistics actors
- CERT/CSIRTs network
- Insurance, Shipping and Cybersecurity companies/enterprises
- European and International organizations & networks for cybersecurity

Cyber-MAR User Requirements

User Requirements extraction methodology

User requirements classified in categories:

- Cyber-security
- Visualization
- Notification
- Audit
- Architecture
- Data security
- Training
- Legal

Co-design of the requirements with the Cyber-MAR stakeholders community:

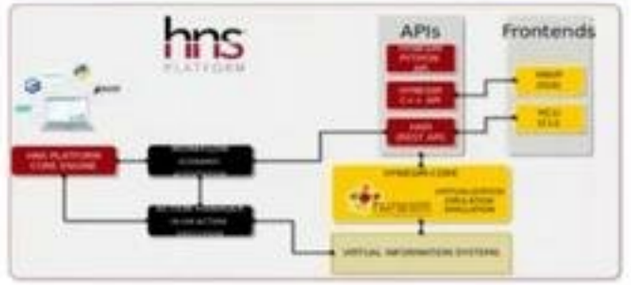
- dedicated workshop in Piraeus
- relative interviews for each pilot area

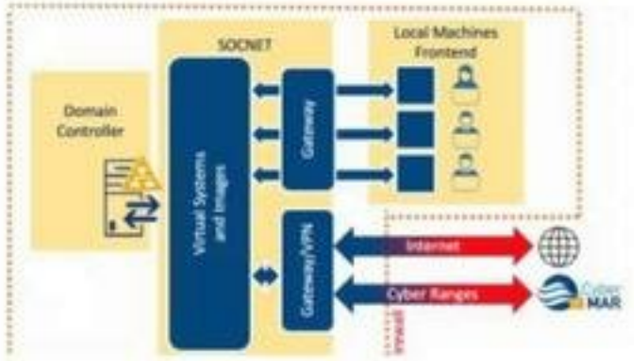
Cyber-MAR System Requirements

- **The categories of the system requirements created are:**
  - **Common**: Horizontal requirements related to most or all components of the Cyber-MAR system
  - **Simulation building**: related to setting up a new simulation instance
  - **Simulation execution**: related to the realization of a simulation
  - **Simulation monitoring**: related to the monitoring of simulation and scenarios during their execution
  - **Risk Analysis & insurance Model**: related to the cybersecurity risk analysis and the econometric model components
  - **Evaluation**: related to the evaluation of trainees
  - **Training**: related to features dedicated to training use cases

Cyber-MAR Components

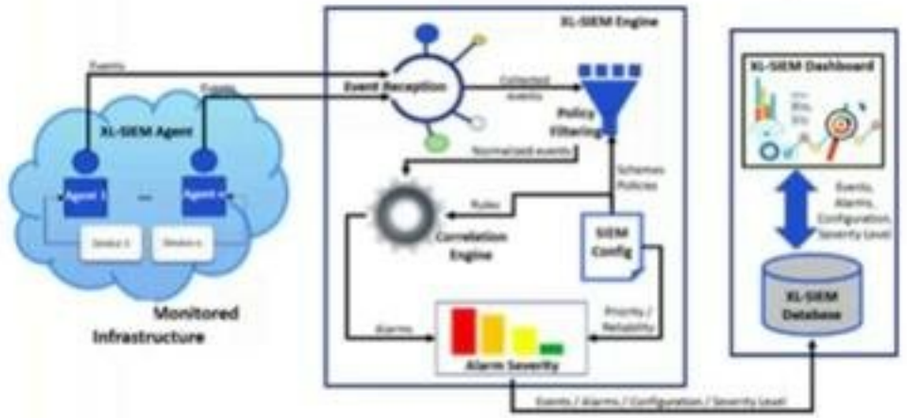
- **HNS**
  - Cyber Range with virtualization and task automation capabilities creating a realistic environment used for training or prototyping computer networks.
- **Ship Simulator**
  - The ship simulator provides the capability to simulate a complete ships bridge (i.e. ECDIS, Radar etc). The simulator can be used to simulate a fully operational ship and traffic flowing between different components can be captured and used for off-line analysis.
- **IDS**
  - Intrusion Detection / Prevention functionality suitable for the maritime scenario. It analyses all relevant network traffic in the scenario and alerts when an attack or other suspicious behavior is detected.
- **Expert SA - High Level SA**
  - Expert Situational Awareness (SA) producing situational awareness visualization of the outputs of network monitoring tools. This view displays detailed technical views with the possibility to dig in to details.
  - The Metric Visualization System (MVS) is a tool for designing and monitoring the security of information systems and increasing the meaningfulness of security metrics by visualizing their full range.



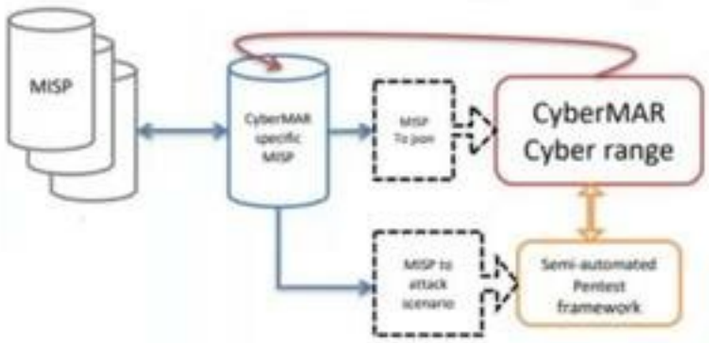


Cyber-MAR Components

- **XL-SIEM and L-ADS**
  - **XL-SIEM:** Real-time collection and analysis of security events. Prioritization, filtering and normalization of the data gathered from different sources. Consolidation and correlation of the security events and generation of alarms and reports Execution of countermeasures (scripts) or creation of tickets for further investigating the incident
  - **L-ADS**: live anomaly detection system based on unsupervised machine learning algorithms that analyses the network traffic using NetFlow to identify anomalous behaviors in device communications

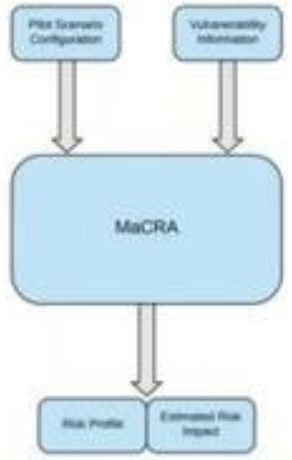


- **CERT**
  - The CERT component is mainly based on technical and operational datas produced by inter-CERT cooperation. Main function is to upgrade the cyber security cooperation MISP platform by setting up and taking part in a MISP community dedicated to the maritime sector stakeholders. This community will allow to share and communicate IOCs and specific maritime consequences of vulnerabilities to improve cybersecurity early warning.



Cyber-MAR Components

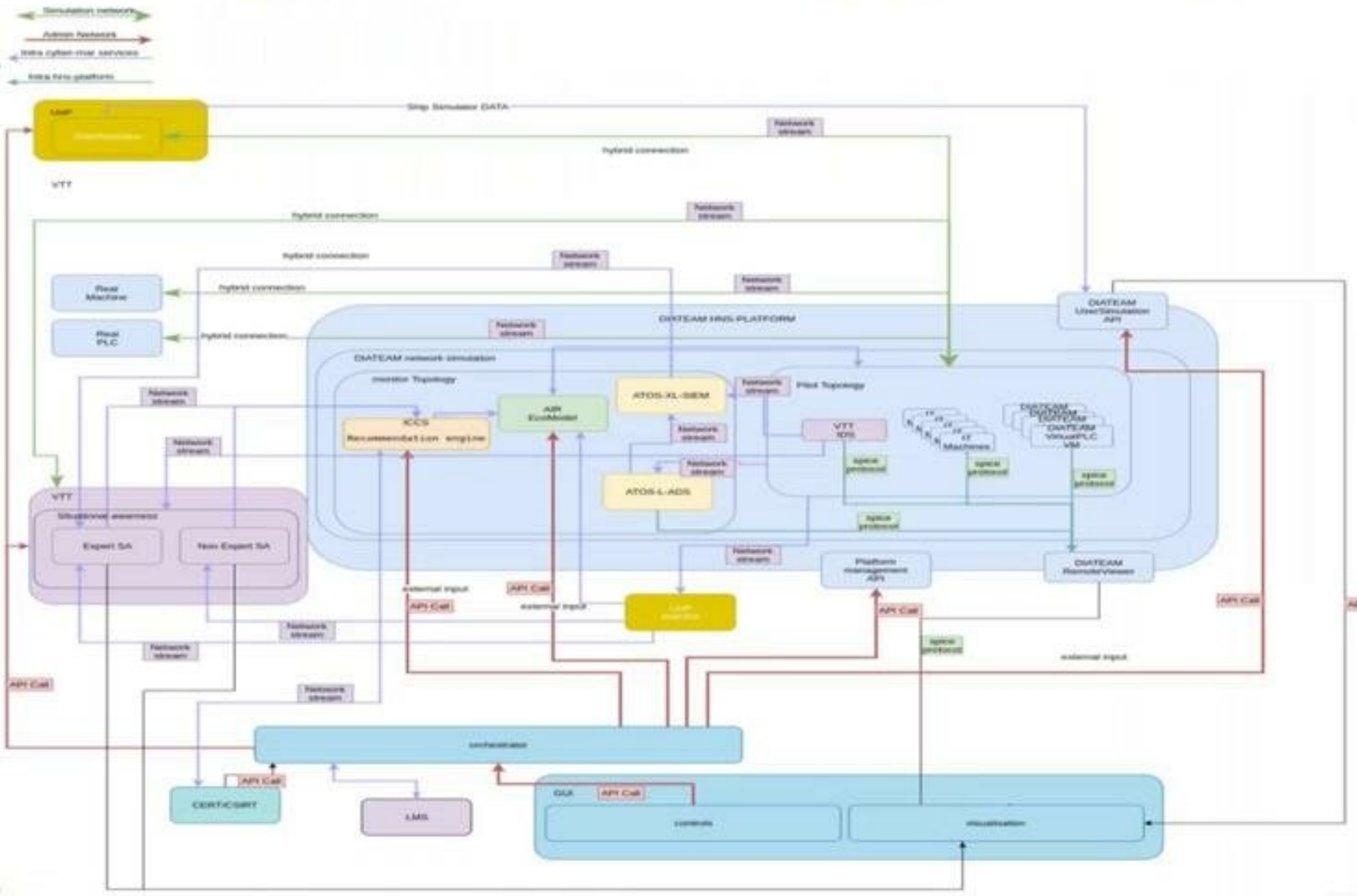
- **Macra**
  - measures the level cyber-risk exposure of the pilot systems under consideration. A risk model is then be applied to a discrete event simulation model of the port operations so that an estimate of the expected effect of cyber-attacks on maritime operations can be calculated.
    - e.g. the effect of the attack will be quantified in terms of the expected reduction in operational capacity of the maritime port and the consequential estimated delay in processing containers that will be caused by that drop in operational capacity.



- **Econometric Model (AIR)**
  - outputs the economic losses for different nodes in the value chain. Either in-terms of business disruption days or monetary losses

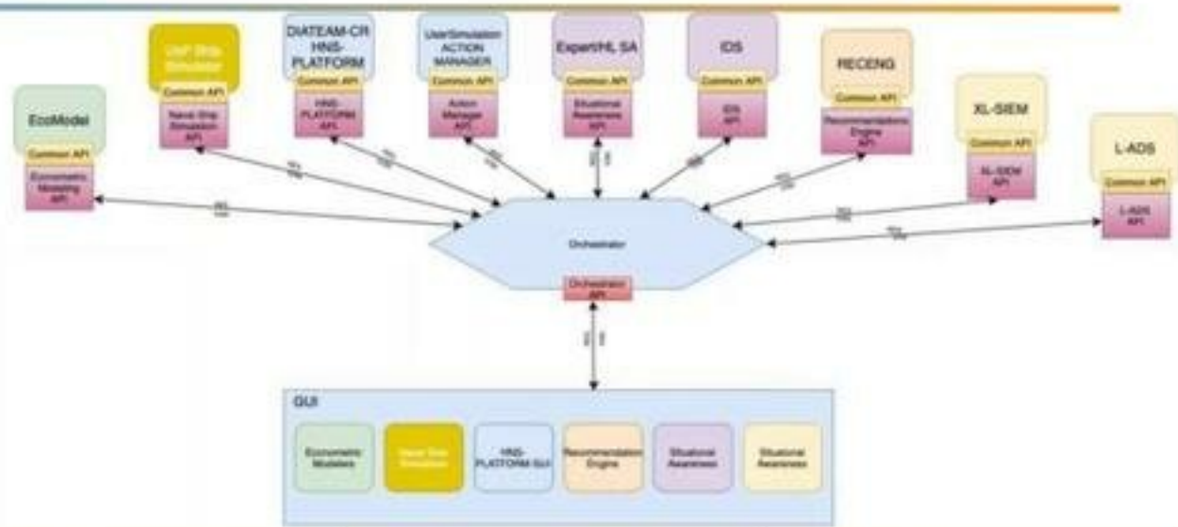
- **Recommendation Engine**
  - receives input from the IDS in terms of the up-to-the-moment sequence of an attacker's actions and overall state of the network. Provides a probabilistic prediction of the next/future actions of the attacker and/or the next/future state of the network. Fused with information from econometric models, aiming to help the defenders prioritize their responses.
- **LMS**
  - Platform to improve performance, skills and retain the best talent in the teams and allows to manage the transformation in e-learning and the distribution of courses

Cyber-MAR High Level Architecture (Physical View)



Cyber-MAR Orchestrator

- The Orchestrator is the main controller component of the Cyber-MAR CR system.
- The Orchestrator controls all other modular components and communicates with them, via an API designed with the principle of functionality inheritance:
  - "all components that wish to integrate with the CR, need to properly implement an API for common, type specific and component specific functions."
- on-going work is started on the specific definitions of the component's API



API Level	Required	Stability
Level 0 - Common API	Yes, without it a component cannot be integrated inside Cyber-MAR	Designed by system architects, changes only between system version changes
Level 1 - Component Type API	Yes for components that provide specific type of service (e.g. SIEM)	Designed by system architects, changes only between system version changes
Level 2 - Component Specific API	No	Designed by developers of components, can change between releases without keeping the same design

Cyber-MAR 1st Pilot

Valencia Pilot Event (conducted **online),** on **16.12.2020**, at **10.00-13.00 CET**, via an online conference platform.

Testing and validating an initial version of the Cyber-MAR system in the scope of a cyber-attack scenario on the port authority's electrical grid, in the **Port of Valencia**.

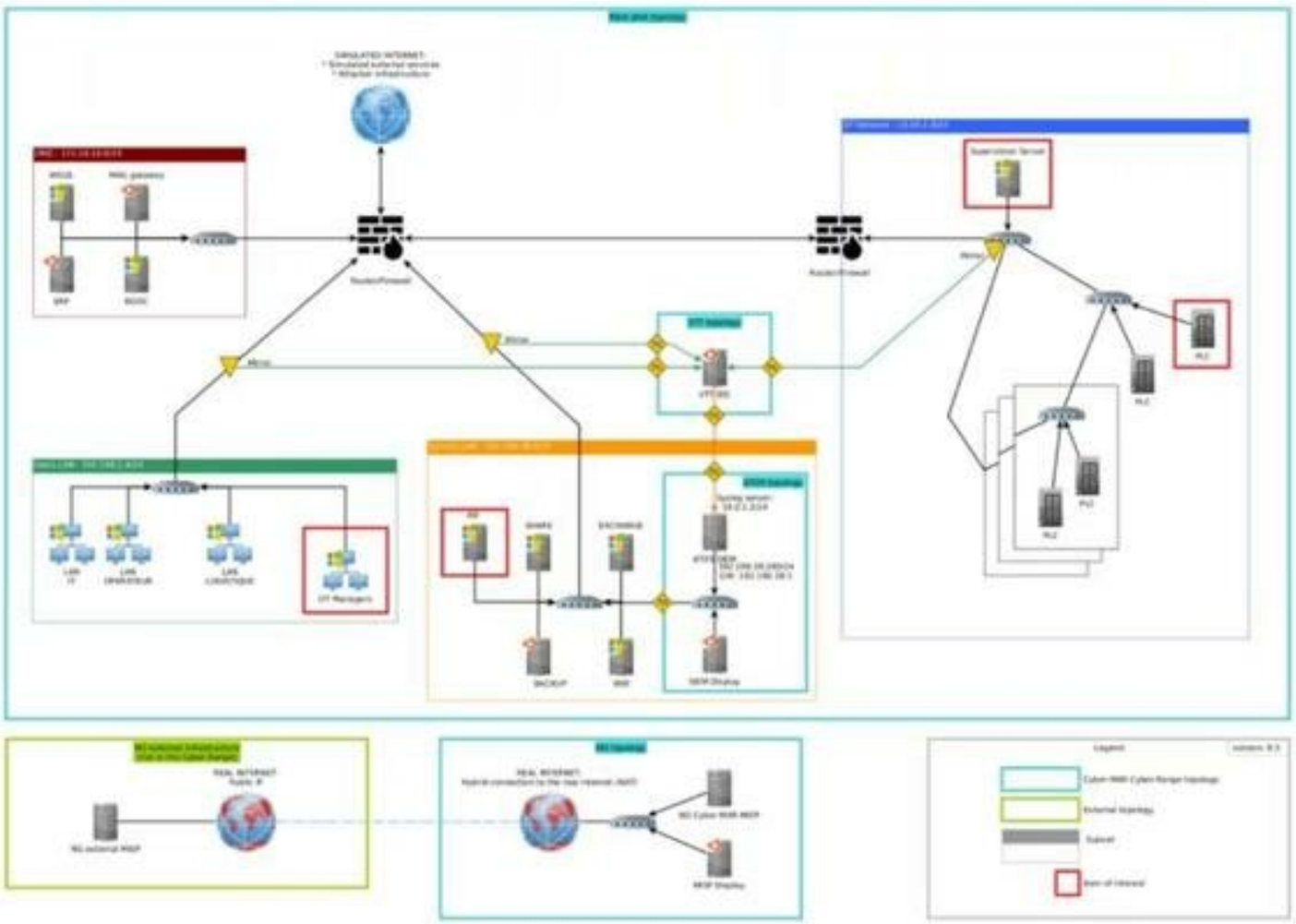
Simulation of a remote access attack on the IT and OT infrastructure, and energy grid.

- cut off the power supply to the port, by shutting down the grid management OT system.
- simulate a Ransomware attack triggered by the Command & Control server, that will cryptolock all workstations within the infrastructure of the port

Registration is free of charge but required.
Please use the link to register and receive the connection details!

https://www.eventbrite.com/e/cyber-mar-valencia-pilot-event-tickets-127998062651

Cyber-MAR 1st Pilot



Scenario Steps:

1. Spear phishing email sent to the OT operator containing malicious document with embedded malicious code (macro)
2. Exploit the Zerologon vulnerability (CVE 2020-1472) to gain access to the Domain Controller (Active Directory) – privilege escalation.
3. Threat actor objectives:
   1. Attacking modbus PLC: Change state from RUN to STOP without authentication
   2. Cryptolock: encrypt files on the machines and network shares and hold them for ransom

Registration is free of charge but required.
Please use the link to register and receive the connection details!

https://www.eventbrite.com/e/cyber-mar-valencia-pilot-event-tickets-127998062651

www.Cyber-MAR.eu

Cyber_MAR

Cyber-MAR EU Project

Cyber-MAR

info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION

Eleftherios Ouzounoglou, ICCS

eleftherios.Ouzounoglou@iccs.gr

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement No. 833389

CYBERWISER.eu

Cyber Range & Capacity Building in Cybersecurity

Niccolò Zazzeri

Trust-IT Services

The CYBERWISER.eu project

Cyber Range Network Joint Webinar

Co-funded by the European Commission
Horizon 2020 – Grant # 786668

CYBERWISER.eu, in a nutshell

- An **H2020 Innovation Action** aiming to become the EU's reference, authoritative, independent ***cyber range platform for professional training***.
- From September 2018 through February 2021.
- Featuring an **open pilot stream**, for you to get to use the CYBERWISER.eu platform (for free!) – Book your own pilot at https://cyberwiser.eu/content/open-pilot-stream

Our main end user targets

1. Cybersecurity students at IHEs and Early Career Professionals

2. SMEs and Mid-caps

3. Large Enterprises and Operators of Critical Infrastructures

4. Public Sector Organisations

CYBERWISER.eu Objectives

Deliver a European Platform for cybersecurity professional training

3 full-scale pilots in key vertical markets & education and activate and manage the “Open Pilots Stream”.

Innovative cybersecurity training tools and materials

Develop a sustainability model for the CYBERWISER.eu training platform.

Create robust & insightful economic models for monetary exposure assessment to risk in virulent cyber climates

Develop and run the "Cybersecurity Professional Register” to promote cybersecurity capacity building in Europe

Contribute to the continuous development of a cybersecurity culture across EU society.

CYBERWISER.eu Training Offer

PRIMER

- Created for students or beginner-level professionals.
- At the primer offering level you can experience the CYBERWISER.eu **e-learning & communication tools such as Web Portal, Cross-Learning Facilities.**
- The Primer Offering Level gives you an **overall introduction to the cyber-risk analysis process.**
- The topics covered within this offering level are the **most common threats like phishing, ransomware and some cases of data leakage.**
- Additional topics to be covered are best practices on reducing insider threats and how to manage and set passwords.

BASIC

- Created for professionals that already know the basic concepts and best practices of cybersecurity.
- The basic Offering Level lessons include a structured approach to identifying and documenting security assets and cyber risks.
- CYBERWISER.eu cyber range environment **includes a wide amount of high realistical practical simulations.**
- At the basic offering level **you can experience training scenarios composed by up to 10 elements.**
- A **set of monitoring sensors.**
- A **basic limited suite of pre-defined attack scripts.**

INTERMEDIATE

- Created for expert users from business context as SMEs or Large Enterprises as well as Public Sector.
- Within the intermediate Offering Level are developed also aspects of **context establishment, cyber-risk assessment, cyber-risk treatment, and cost/benefit analysis not covered at the Basic level.**
- At this level are available **training scenarios composed by up to 50 elements.**
- A set of **monitoring sensors tailored to specific exercises,**
- A **full suite of pre-defined attack with suggestions of possible countermeasures.**
- A **set of models that may be executed by Economic Risk Evaluator are also available.**

ADVANCED

- Created for large organisations or public administrations that have more advanced cybersecurity training needs.
- The advanced Offering Level covers all aspects of context establishment and cyber-risk assessment, as well as cyber-risk treatment and cost/benefit analysis.
- At this level are available **training scenarios composed by up to 500 elements.**
- The Digital Library offers a **full choice of virtual templates and the possibility of creating new ones.**
- A **set of monitoring sensors tailored to specific exercises,**
- A **full suite of pre-defined attack with suggestions of possible countermeasures.**
- **The risk assessment algorithm produces risk levels in terms of economical loss given that the risk materializes.**

3 Full Scale Pilots supporting validation

Energy Generation And Distribution

Railroad Transport

Professional And Academic Training

Practical use cases application in FSPs

Academic Pilot

- SQL Injection
- Firewall and Network Filtering
- Network and Vulnerability Scan
- Idle Scan
- Privilege Escalation
- AppArmor Defense
- Session Hijacking

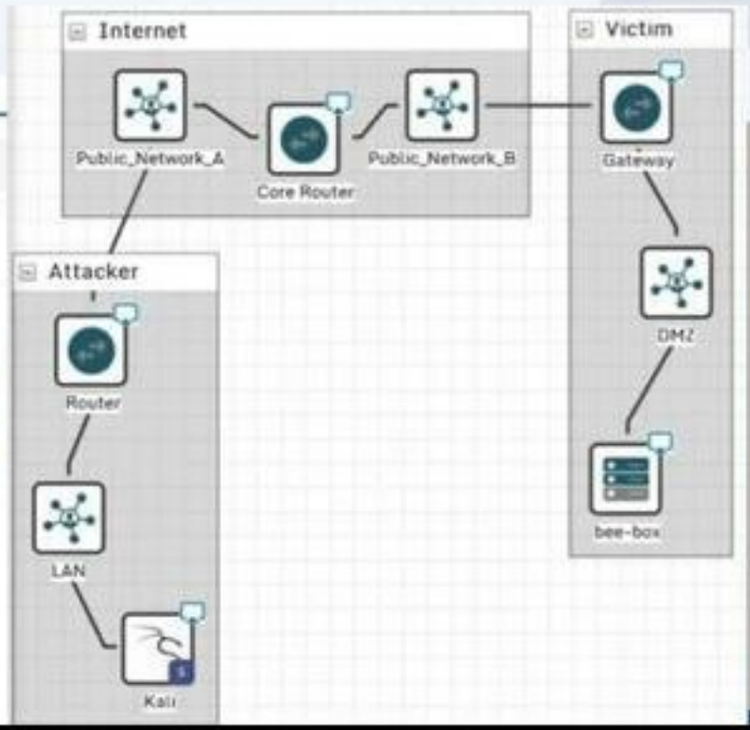
Transport Pilot

- SQL Injection
- Phishing attack
- Password Cracking
- Red team vs Blue Team (TBD)

Energy Pilot

- SQL Injection
- Cross-Site Scripting
- Phishing Attack
- Targeted Malware
- Power outage

CYBERWISER.eu Training Path



Opportunity: the Open Pilots Stream

Open Pilots Stream

- Train your staff for free!
- Fully customizable cyber training to meet your cybersecurity needs
- Get access to one of the most advanced Cyber Range platforms in the world

What is it?

An Open Pilot is your opportunity to train your staff in cybersecurity, for free, on the CYBERWISER.eu Capacity Building Cyber Range Platform. You will benefit from a customisable learning path based on your organisation's needs!

Who is it for?

Our Open Pilot Stream is dedicated to **SMEs, Research & Academia, Large Companies** and **any organisation** interested in testing our platform

While our training is directed primarily towards **IT personnel** who need to develop advanced skills in cybersecurity, training pathways have also been created for **individuals** from other, **non-technical areas** of an organisation.

How does it work?

It is very easy! All you need to do is following the steps below. Please note that the duration of your Training Pilot will be determined by the customised specifications we agree on. An introductory workshop is the ideal place for these discussions but you can also get the ball rolling by completing the application form here. The average length of an open Pilot is between 3 and 6 months.

- ***Complete the form with the requirements of your own Pilot:***
  https://www.cyberwiser.eu/content/cyberwisereu-open-pilot-scheme
- ***What we will grant you as Open Pilot?***
  - Onboarding package to use the platform (training material and dedicated interfaces)
  - Issued credentials to manage the instantiation of the platform for your specific Pilot
  - Continuous support by our Team

CYBERWISER.eu

Thank you for your attention! *Questions?*

Main contact:

Niccolò Zazzeri, n.Zazzeri@trust-itservices.com

WP6 Leader

www.cyberwiser.eu @cyberwiser

Atos Trust-IT Services SINTEF XLAB Università di Pisa Ferrovie dello Stato Italiane edp Aon RHEA

CYBER RANGES FINAL - Microsoft PowerPoint (Product Activation Failed)

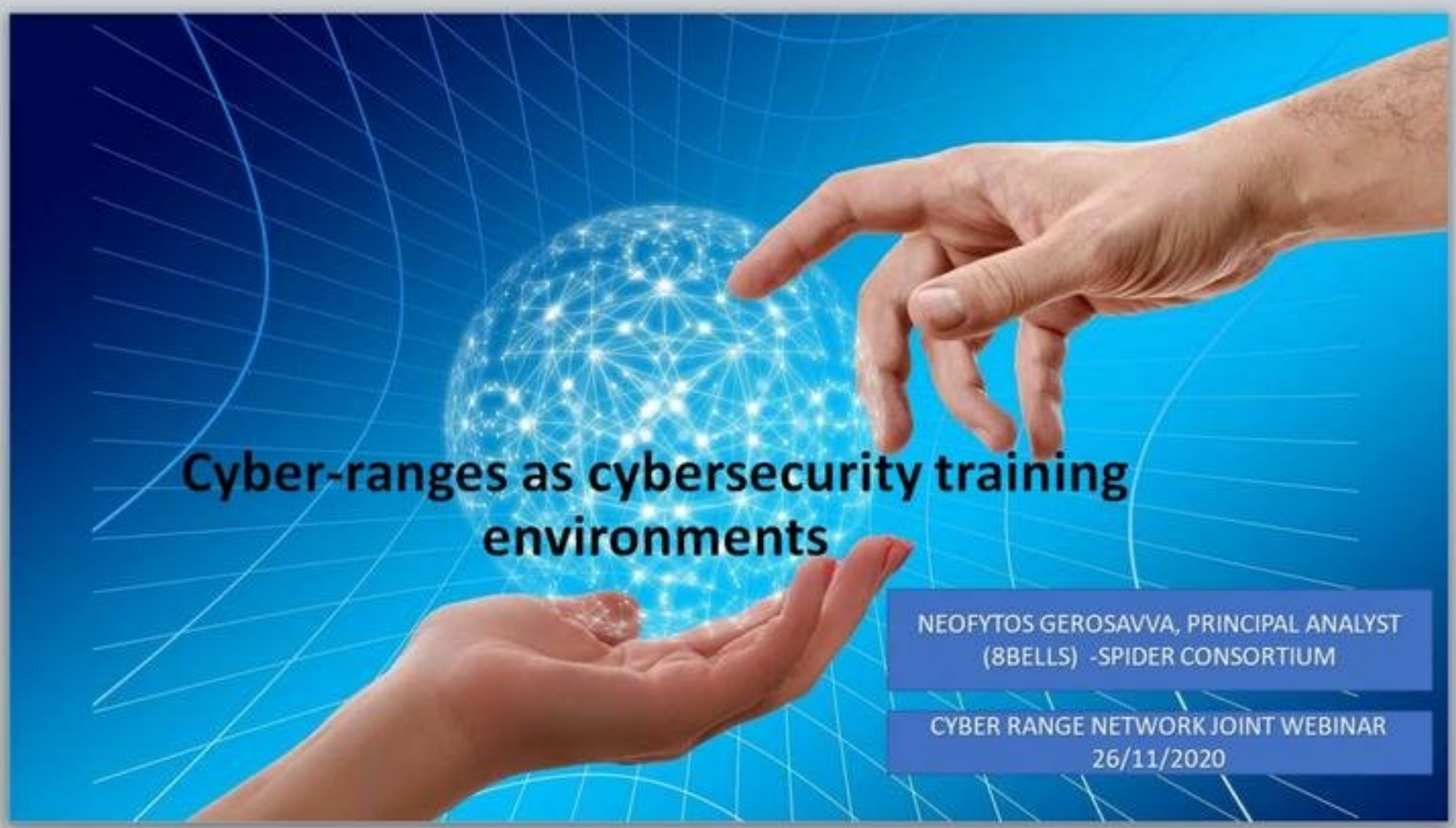
File | Home | Insert | Design | Transitions | Animations | Slide Show | Review | View

From Beginning | From Current Slide | Broadcast Slide Show | Custom Slide Show | Set Up Slide Show | Hide Slide | Rehearse Timings | Record Slide Show | Play Narrations | Use Timings | Show Media Controls | Resolution: Use Current Resolution | Show On: | Use Presenter View

Start Slide Show | Set Up | Monitors

Slide Show From Beginning (F5)

Start the slide show from the first slide.



Slide 1 of 10 | "Office Theme" | English (U.S.) | 69%

Type here to search | ENG | 1:34 PM 11/26/2020

Cyber-ranges as cybersecurity training environments

NEOFYTOS GEROSAVVA, PRINCIPAL ANALYST
(8BELLS) -SPIDER CONSORTIUM

CYBER RANGE NETWORK JOINT WEBINAR
26/11/2020

What is a cyber range?

"A cyber range is a platform for the development, delivery and use of interactive simulation environments. A simulation environment is a representation of an organisation's ICT, OT, mobile and physical systems, applications and infrastructures, including the simulation of attacks, users and their activities and of any other Internet, public or third-party services which the simulated environment may depend upon. ***A cyber range includes a combination of core technologies for the realisation and use of the simulation environment and of additional components which are, in turn, desirable or required for achieving specific cyber range use cases****."*

– European Cyber Security Organisation (ECSO), "Understanding Cyber Ranges from Hype to Reality" (White Paper) rel. 30-March 2020.

Background

- The complex landscape surrounding today's cyber security strengthens the need for better trained and qualified experts securing critical multi-tenant and multi-service environments, such as 5G mobile networks.
- During the last years, the number of cyber-attacks has gradually increased and various recent security incidents worldwide have demonstrated the fact that there is an increase also in the complexity and severity of cyber security threats
- According to 2020 Official Annual Cybercrime Report by Cybersecurity Ventures, sponsored by Herjavec Group, cyberattacks will cost the world $6 trillion annually by 2021, in comparison with the $3 trillion in 2015
- The attackers are becoming more sophisticated and they are using even more advanced methods and techniques.
- As an effect companies worldwide understand the importance of finding new ways,approaches and innovative cyber security models to keep their assets and their infrastructures safe

The Cyber ranges concept

The Cyber ranges concept

- Traditionally, cyber ranges were platforms that enabled commercial companies, government agencies and military organizations to study the effectiveness of their cybersecurity technologies

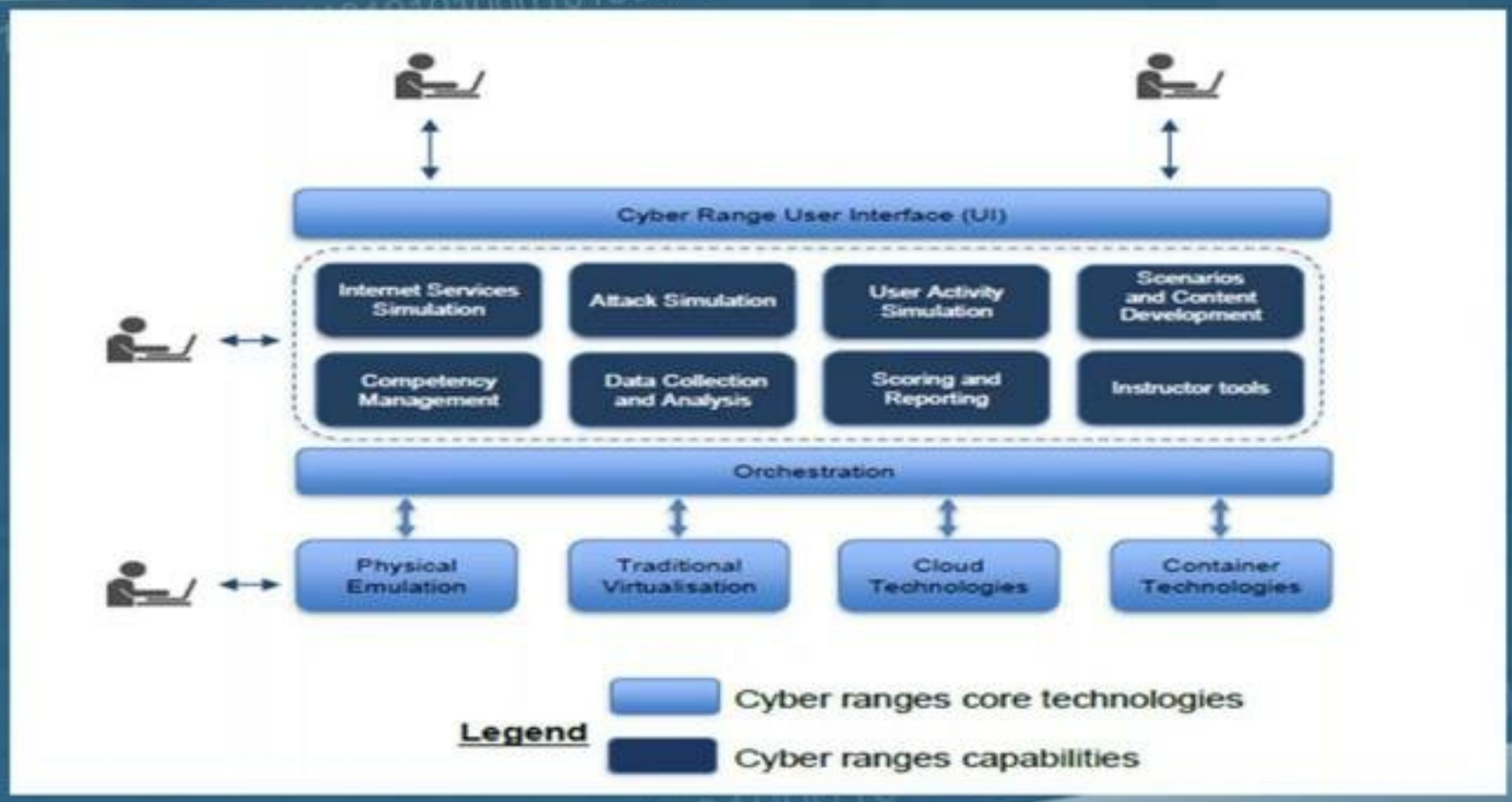
The Cyber ranges concept

- Traditionally, cyber ranges were platforms that enabled commercial companies, government agencies and military organizations to study the effectiveness of their cybersecurity technologies
- These platforms can provide the chance to their potential users to simulate real-world complexity cyber scenarios with high fidelity and train employees and customers on the latest threats through high quality realistic cyber exercises, without endangering the productive environment, which is just replicated virtually.
- A cyber range provides a place to practice correct and timely responses to cyber attacks and the participants can practice skills such as network defense, attack detection and mitigation, penetration testing etc
- At a high level, the two key drivers responsible for the growing demand for cyber ranges are the cementing of cyber as a separate domain of warfare and the development and wide spreading of cloud technology, acting as a major enabler for cyber ranges to develop.

Benefits of Cyber Range Solutions

- Providing the experience of real-world threats /cyberattacks in a safe and well controlled environment
- Because of their ability to represent real-world cyber threat scenarios in a virtual environment, they also present an opportunity to enhance organizational training capabilities
- Provide the opportunity to various type of organizations to test their infrastructures and identify and assess potential vulnerabilities.
- Software developers can use cyber range applications to validate virtual Proof of Concepts.
- Cyber ranges come equipped with sets of gamified elements providing all potential benefits of gamification in learning
- Offer a simulated environment with real time feedback where teams can work and train together to improve their capabilities
- An efficient way for trainees to gain practical knowledge through hands on activities
- By facilitating high-fidelity simulations, they can improve stability, security and performance of cyberinfrastructures

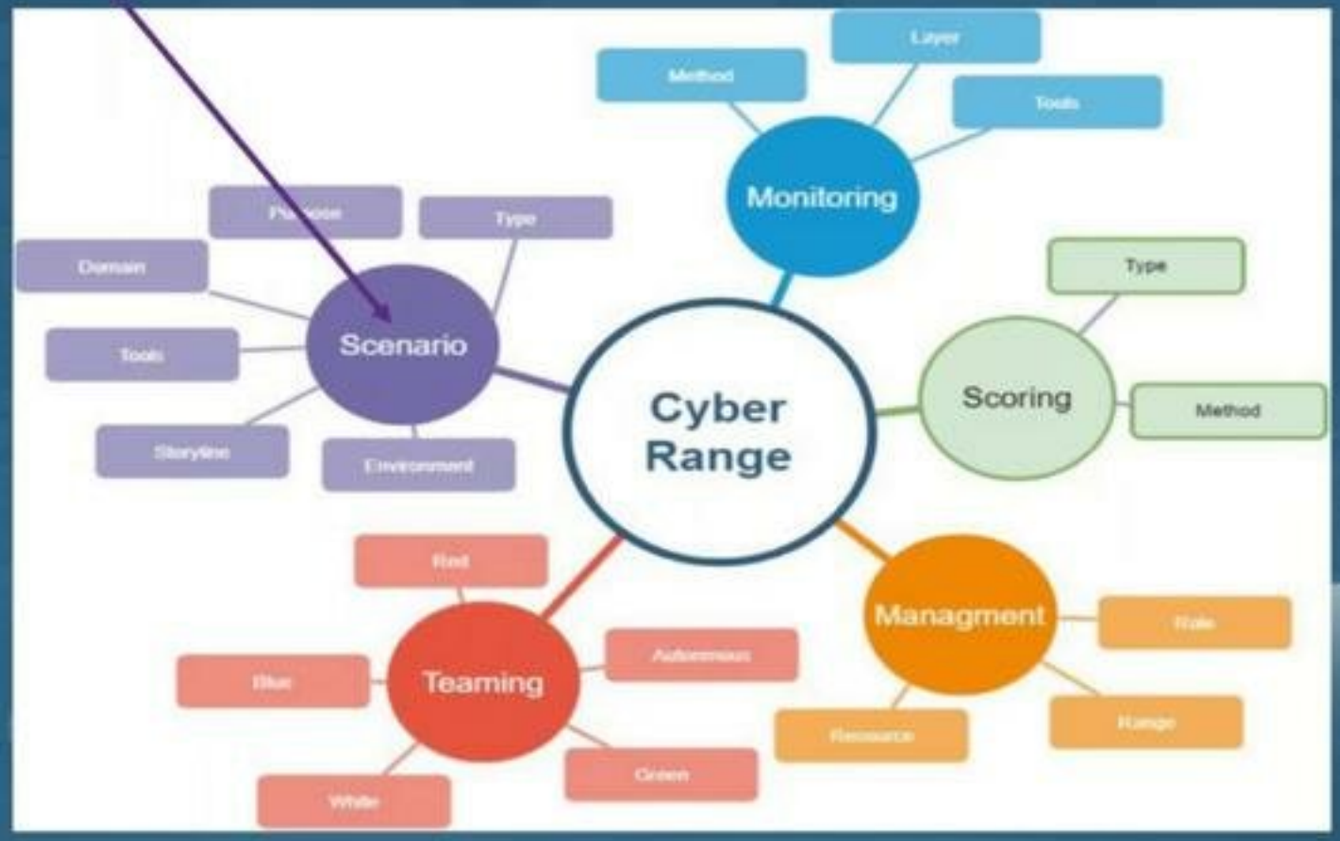
Cyber Range Functionalities



By definition, a cyber range does not need to include all or any of the scheme capabilities. The difference between cyber ranges lies primarily in the amount of work required for each cyber range to deliver specific use cases..

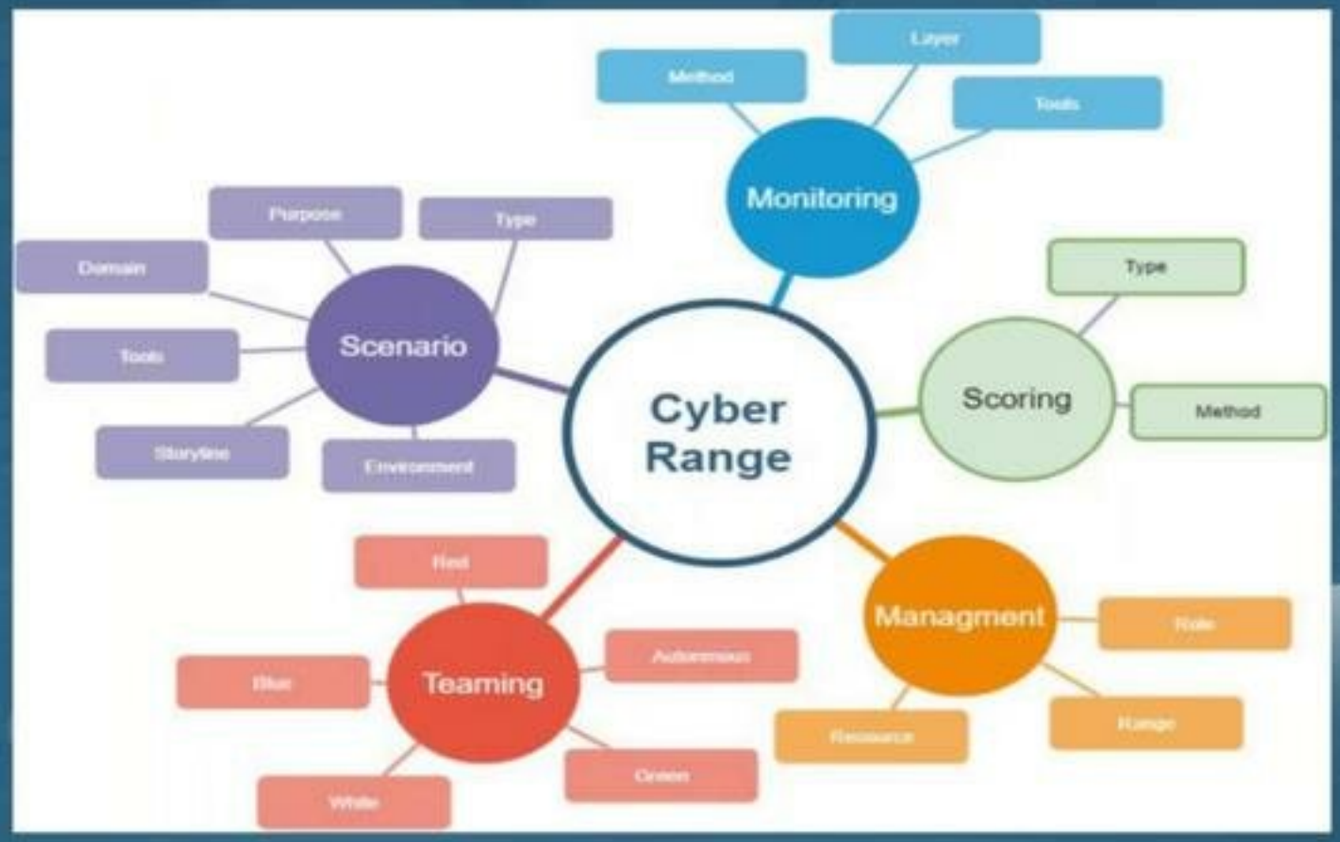
TAXONOMY

Scenarios define the execution environment as well as the storyline that indicates the execution steps of a test or a training exercise.



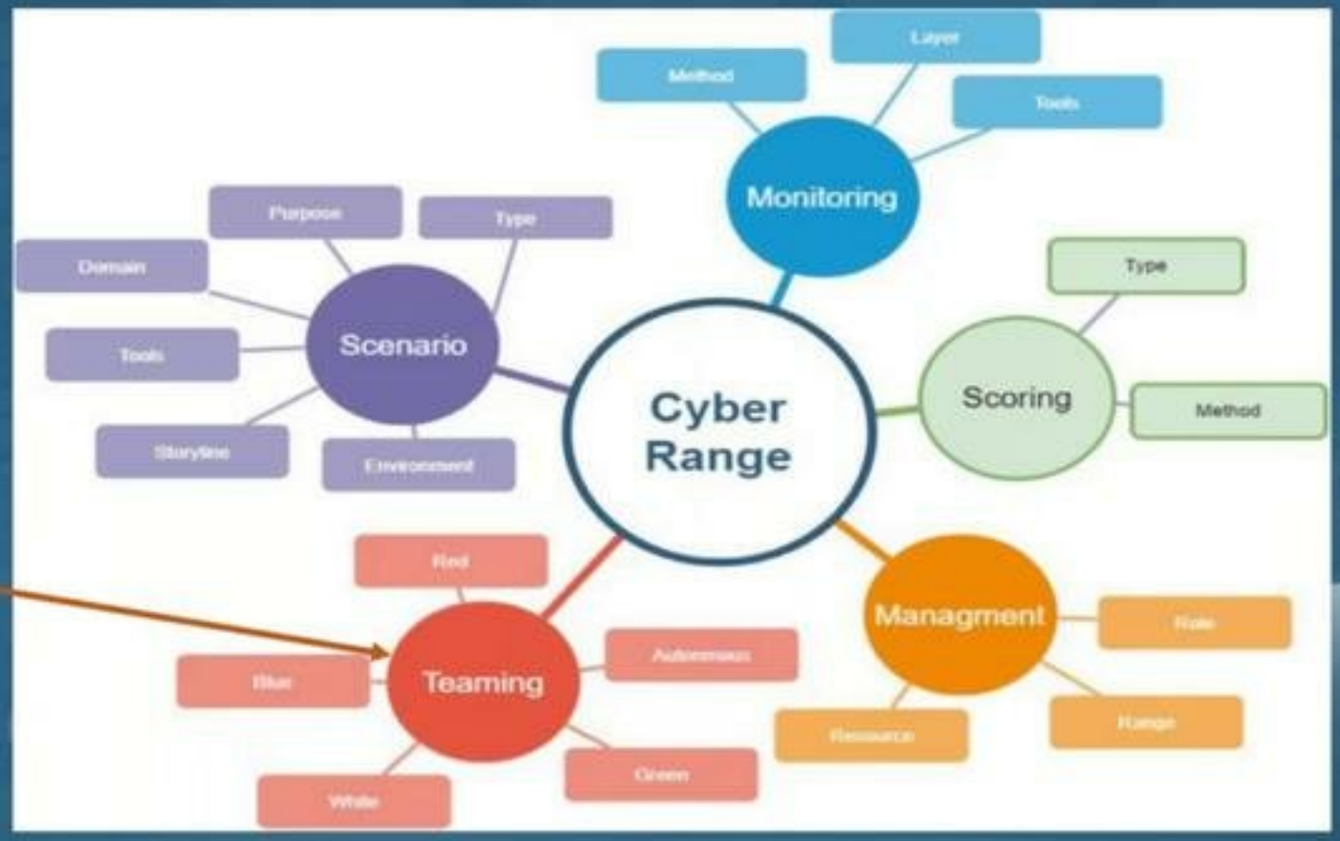
TAXONOMY

Monitoring includes the methods, the tools and the layers at which real time monitoring of cyber security exercises and tests are performed

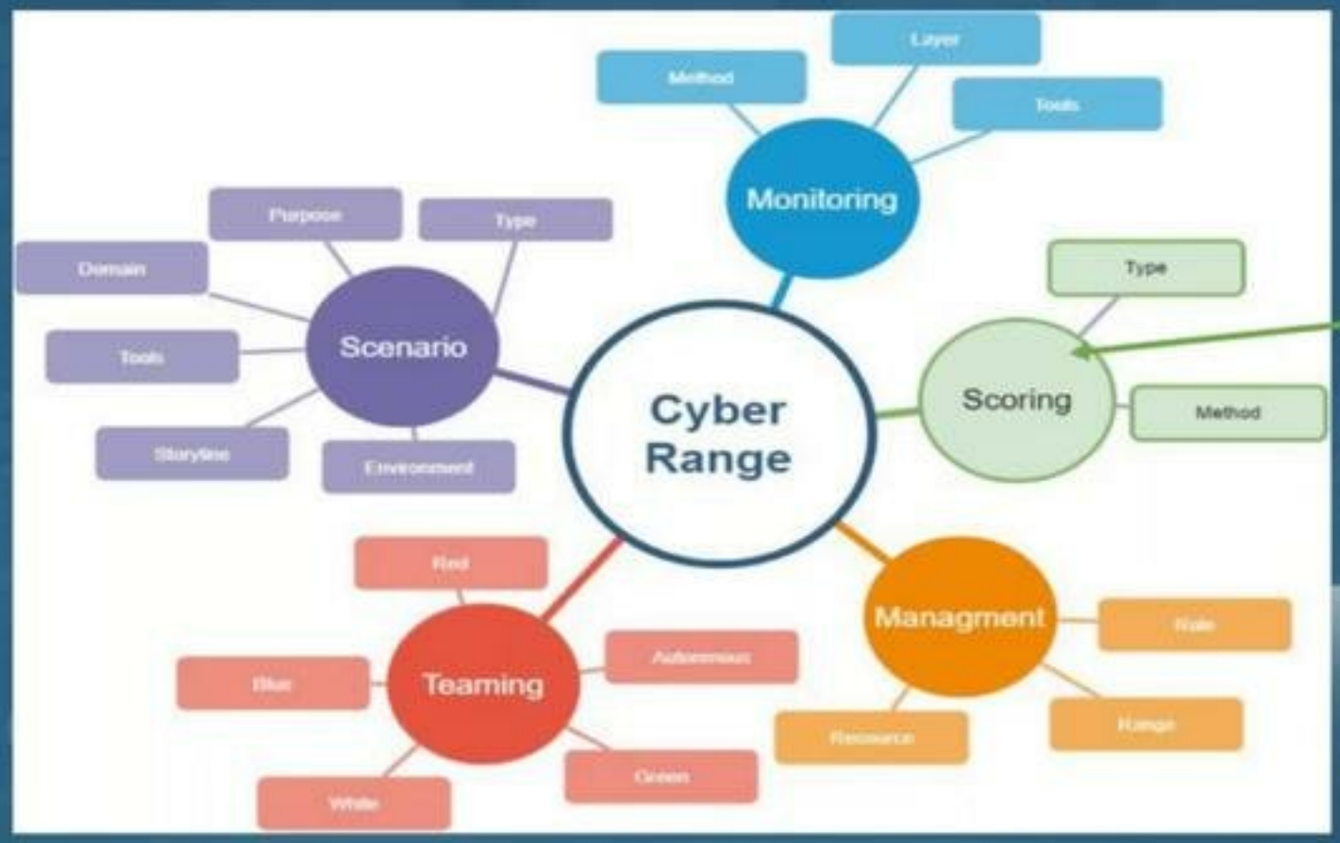


TAXONOMY

Teaming includes an individual and a group of individuals that design, develop, manage and participate in a cyber security exercise or a test



TAXONOMY



Scoring uses data from monitoring systems in order to give performance related semantics to the low level technical events observed during monitoring of cyber security exercises and tests.

TEAMING

Green team is responsible for the development, monitoring and maintenance of the exercise infrastructure designed by the white team.

Yellow Teams software builders and application developers , generating legitimate network traffic which can be used by red and blue teams in attack and defense.

Blue team ,threat hunters, responsible to identify and patch potential vulnerabilities that can be exploited by a red team.

Red team – ethical hacking, cyber security adversaries are modeled to exploit potential vulnerabilities

White team designs the exercise and experiment scenario, objectives, rules and evaluation criteria. They set a set of rules of engagement between red and blue team

Purple teams perform the communication role between multiple exercises teams. They do information sharing to increase the exercise effectiveness and facilitate improvements

SHOW TASKBAR | DISPLAY SETTINGS | END SLIDE SHOW

GoToMeeting is using the webcam

Swap Presenter View and Slide Show

Duplicate Slide Show

0:00:04 | 13:46

Slide 1 of 5

Next slide

No Notes.

GoToMeeting
is using the webcam

Common Collaboration Ground and Next Steps

Common View

- **Cluster activities** have evolved as a fruitful and effective way to encourage collaboration among various organizations and to facilitate the efficient exchange of knowledge between them.
- Through the formulation of collaboration hubs, European funded projects, have the opportunity to **gain knowledge** and **interact** with the other parties, as well as to build on each other's results over time.
- Clusters enable the involved projects to **share data, findings and results** among them, **exchange rapid feedback** on research activities, and reach a wider audience to communicate and promote their outcomes through the expansion of their individual networks.
- In the context of such **innovation clusters**, projects can follow a **co-creation approach** and evaluate work as it progresses, address common issues, and implement common strategies for further improvements.
- Such actions can be effectively supported and further promoted through the organization of joint events such as conferences, webinars, workshops etc.

Common View

FORESIGHT, SPIDER and Cyber-MAR projects have a lot in common:

- **their philosophy**
- **basic objectives**
- **concept and vision.**

Each one of these projects is involved in the implementation of innovative cyber-range platforms, aiming to **upgrade their end users' skills**, increase **cyber awareness** and **preparedness level**, improve **cyber-threat training** and at the same time aim to **offer reliable and advanced econometric and risk analysis tools**.

FORESIGHT, Cyber-MAR and SPIDER are united towards their vision to raise awareness on cybersecurity and promote the use of cyber ranges.

Initiated a collaboration, aiming to expand it throughout the three projects' lifetime.

Next Steps

Additional Webinars

- Organization of workshops on special issues

Shared - collaborative training activities

- expansion of content with other project use-cases

Homogeneous KPI framework

- For educational parts of the platforms

THANK YOU FOR YOUR ATTENTION

Eleftherios Ouzounoglou, ICCS

eleftherios.ouzounoglou@iccs.gr